Universidad
Carlos III de Madrid

INGENIERÍA TÉCNICA EN INFORMÁTICA DE GESTIÓN
DEPARTAMENTO DE INFORMÁTICA
PROYECTO FIN DE CARRERA

Adaptación de una empresa tecnológica a UNE-ISO/IEC 27001 (versión 2013)

Autor: Javier Donoso Morán
Tutor: Miguel Ángel Ramos González
Leganés, octubre de 2015

Título: Adaptación de una empresa tecnológica a UNE-ISO/IEC 27001 (versión 2013)
Autor: Javier Donoso Morán
Tutor: Miguel Ángel Ramos González

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día __ de _____ de 20__ en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

Primeramente, me gustaría agradecer a mi tutor su ayuda en esta empresa por su predisposición y por realizar este trabajo para conmigo de manera tan abnegada en su nueva etapa en la vida.

A mi familia, en especial a mi madre, por su amor infinito y desinteresado y para que no se preocupe más por este tema. Mamá¡¡¡¡¡¡ Ya lo he acabado ☺

A mis amigos, que entre unos y otros siempre han estado ahí en todos los momentos de mi vida y, en este momento, yo no me puedo olvidar de ellos. (Víctor, el año que viene vamos a tu pueblo no te preocupes).

A Álvaro, porque sin ti esto no hubiera sido posible. Volvería ahora mismo a los años que convivíamos diariamente. Eres un jefe, ya lo sabes ;)

A Pérez, por su ayuda a la hora de realizar este proyecto con la lengua de Shakespeare. Una vez más, me has demostrado la calidad de persona que eres ;).

A toda la gente que ha pasado por mi vida que, por circunstancias, ya no forma parte de ella y que en mayor o menor medida han aportado su granito de arena para que consiguiera ser quien soy.

Y por último y no por ello menos importante a Mayra, porque sé, que a su manera, me ha apoyado para que pudiera terminar esto y aunque no me lo dijera, estaba preocupada por mí. Te quiero cariño.

Resumen

En la primera parte de este trabajo se detalla la introducción y los objetivos del proyecto. También se ahonda en las bases de lo que es un Sistema de Gestión de la Seguridad de la Información, lo que representa, que objetivos, recomendaciones y requerimientos son necesarios tener definidos, así como algunos ejemplos de políticas de seguridad. Se expone el sistema CIA y su importancia en un SGSI. Todos estos conceptos, se completan con una breve descripción de algunas de las normas internacionales ISO más representativas, haciendo especial énfasis en la norma 27001, que es la base del proyecto.

Para la segunda parte y como centro del proyecto, se ha creado una guía que puede servir de referencia a una empresa que desee certificarse en la norma ISO 27001, ya que se ha desarrollado un manual de seguridad siguiendo la estructura de la norma 27001:2013, en la que se describe, punto por punto, todos los requisitos que impone dicha norma, así como todos los registros y documentos que hay que crear para poder obtener la certificación.

Abstract

On the first part of the Project it is detailed the abstract, and purpose of it. It also deepens on the fundamentals of what an ISMS is, what it represents and the goals, recommendations, and requirements that must be defined as well as security policies that are implied. It is explained the CIA system, and it´s importance on a ISMS. All these concepts are completed with some short descriptions on some of the most relevant international ISO Standards focusing on the 27001 Standard, which is the core of the project.

For the second part and as the center of the Project it has been created a manual that may be used as a handbook for an enterprise that is willing to get certified on the ISO 27001, given that it has been created following the 27001:2013 guidelines. The final result is a guide that will serve as complete assistance to get all the registries, tasks and requirements that getting certified demands.

INDICE

CAPÍTULO I: Introducción y objetivos

1. Introducción 6
2. Objetivos 14
   2.1. Objetivo general 14
   2.2. Objetivos específicos 14
3. Estructura de la memoria 14

CAPÍTULO II: Fundamentos

1. Seguridad de la Información 17
2. Sistema de Gestión de la Seguridad de la Información (SGSI) 18
   2.1. Algunos conceptos de un SGSI 20
      2.1.1. Activos 22
      2.1.2. Eventos e Incidentes en la seguridad 24
      2.1.3. Amenaza 26
3. Gestión de la Información 27
   3.1. Ciclo de Vida de la Seguridad de la Información 30

CAPITULO III: Normas y Estándares

1. Definiciones 32
   1.1. Normas 32
   1.2. Estándares 32
2. Esquema Nacional de Seguridad 33
3. Serie de normas 27000 36
4. Norma ISO 27001 44
   4.1. Cambios en la versión 2013 48
   4.2. UNE-ISO/IEC 27002:2014 55

CAPITULO IV: Proceso de certificación de la norma 27001 en una organización

1. Proceso de adaptación a la norma ISO 27001 58
   1.1. Objeto 58
   1.2. Ámbito de aplicación 58
   1.3. Objetivo 59

1.4. Definiciones 60
1.5. Documentación del SGSI 67
1.6. Presentación de la empresa 69
1.7. Contexto de la organización 69
1.7.1. Comprensión de la Organización y su contexto 69
1.7.2. Comprensión de las necesidades y expectativas de las partes interesadas 70
1.7.2.1. Cumplimiento de Requisitos Legales 70
1.8. Alcance – SGSI 71
1.8.1. Requisitos Generales 71
1.8.2. Procesos 71
1.8.3. Ubicaciones 72
1.8.4. Tecnologías 72
1.8.5. Requisitos legales 73
1.8.6. Partes interesadas 73
1.8.7. Exclusiones 73
1.9. Sistema de Gestión de Seguridad de la Información 73
1.10. Liderazgo 74
1.10.1. Liderazgo y compromiso 74
1.11. Responsabilidad de la Dirección 74
1.11.1. Compromiso de la Dirección 74
1.12. Política de Seguridad de la Información 75
1.13. Funciones, Responsabilidades y Autoridades 77
1.13.1. Responsabilidad y Autoridad 77
1.13.2. Representante de la Dirección 77
1.14. Planificación 78
1.14.1. Acciones para abordar los riesgos y oportunidades 78
1.14.2. Gestión del Riesgo de la Seguridad de la Información 79
1.14.3. Tratamiento de los Riesgos de Seguridad dela Información 80
1.14.4. Objetivos de Seguridad y planes para alcanzarlos 80

1.15. Gestión de los Recursos 81
1.15.1. Provisión de Recursos 81
1.15.2. Recursos Humanos 82
1.15.2.1. Generalidades 82
1.15.2.2. Competencia 83
1.15.3. Concienciación 84
1.15.4. Comunicación 84
1.16. Requisitos de la Documentación 85
1.16.1. Generalidades 85
1.16.2. Manual de Seguridad 86
1.16.3. Control de documentación y registros 86
1.17. Operación 87
1.17.1. Planificación, Operativa y Control 87
1.17.2. Operación: Análisis del Riesgo de la Seguridad de la Inf. 88
1.17.3. Operación: Tratamiento del Riesgo de la Seguridad de la Inf. 89
1.18. Evaluación del desempeño 89
1.18.1. Generalidades 89
1.18.2. Medición y Seguimiento 89
1.18.2.1. Auditorías internas 89
1.18.2.2. Seguimiento y Medición de los Controles 90
1.18.2.3. Seguimiento y Medición de Objetivos 90
1.18.3. Análisis de datos 90
1.18.3.1. Auditorías Internas del SGSI 90
1.19. Revisión por la Dirección 91
1.19.1. Generalidades 91
1.19.2. Información para la revisión 91
1.19.3. Resultados de la revisión 92
1.20. Mejora 93
1.20.1. Mejora continua 93
1.20.2. Acciones correctivas 94

2. Declaración de Aplicabilidad (SOA) 94

PLANIFICACIÓN

Planificación de tareas 100

Diagrama de Gantt 101

PRESUPUESTO 102

CONCLUSIONES FINALES

Conclusiones 104

BIBLIOGRAFÍA

Referencias 107

ANEXO I: Modelo PDCA

Planificar: ¿Cómo se decide qué hacer y en qué orden? 111

Hacer: ¿Cómo lo hago? 115

Comprobar: ¿Cómo puedo saber si lo que hice funcionó? 117

Actuación: ¿Cómo puedo decidir qué hacer a continuación? 118

ANEXO II: Programa de Auditoría Interna

Auditoría Interna – Internel 122

INDICE DE IMÁGENES

Imagen 1. Proceso SGSI 20

Imagen 2. Matriz de Entidades 20

Imagen 3. Sistema jerárquico de políticas de seguridad 22

Imagen 4. Matriz de activos 23

Imagen 5. Ciclo de vida de un incidente 25

Imagen 6. Proceso SGSI 30

Imagen 7. Ciclo de vida de la información 30

Imagen 8. Cambios versión 2014 51

Imagen 9. Mapa general de Procesos 72

Imagen 10. Mapa gestión del riesgo 88

Imagen 11. Declaración de Aplicabilidad 98

INDICE DE TABLAS

Tabla 1. Cláusulas ISO 27001 52

Tabla 2. Cambios Anexo A 53

Tabla 3. Controles eliminados en el Anexo A 54

Tabla 4. Nuevos controles en el Anexo A 55

Tabla 5. Requisitos Previos 118

Tabla 6. Lista de buenas prácticas recomendadas 120

1. Introducción

En el momento en el que vivimos actualmente, la seguridad de la información es un concepto que cualquier empresa está (o al menos debería de estar) intentando implantar en su organización debido a la gran cantidad de información que se crea o modifica a diario y de su importancia.

Esto, unido a que hemos convertido el uso de Internet como el eje central de nuestras vidas tanto personal como profesionalmente, ha transformado en imprescindible el hecho de conocer qué recursos de la compañía deben de protegerse para poder así controlar los accesos a los sistemas de la empresa, tanto internos como externos y evitar pérdidas y/o fugas de la información.

Además, hay que tener también en cuenta que por temas legales regulatorios y por la confianza depositada por partes relevantes interesadas (accionistas, inversores, suministradores, empleados, directivos, etc.) en estas organizaciones, son incluso de aplicación obligatoria ciertas leyes como la L.O.P.D. (L.O. 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal) o la L.S.S.I. – C.E. (Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico).

Con la evolución de los sistemas de la información, varios organismos han ido desarrollando ciertas normativas independientes y globales, que tratan de regular la seguridad de la información en las organizaciones empresariales aplicando lo que se denomina: Sistema de Gestión de la Seguridad de la Información (SGSI). Ejemplos de estas normas son:

- S.O.G.P.: Information Security Forum's Standard of Good Practice, basado en las experiencias del Foro de la seguridad de la información (ISF).
- I.S.M.3: Information Security Management Maturity Model, es un estándar de ISECOM para la gestión de la seguridad de la información. Está pensado para mejorar la integración con otras metodologías y normas como COBIT, ITIL o CMMI.
- C.O.B.I.T.: Control Objectives for Information and related Technology) es una guía de mejores prácticas presentada como marco de trabajo, dirigida al control y supervisión de Tecnología de la Información (TI). Está mantenido por ISACA.

- ISO/IEC 27001 es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

Será sobre esta última norma, sobre la que se desarrollará gran parte de este trabajo.

2. Objetivos

2.1 Objetivo general

El objetivo general de este Proyecto de Fin de Carrera es exponer la norma ISO/IEC 27001, detallar los cambios habidos en la versión del año 2014 y, posteriormente, pormenorizar el proceso de certificación en la norma para una empresa tecnológica.

2.2 Objetivos específicos

- ✓ Generar la documentación necesaria para fortalecer el SGSI de la empresa.
- ✓ Realizar una guía que pueda servir para que otras compañías consigan certificarse en la norma ISO/IEC 27001.
- ✓ Presentar el programa de auditoría interna a una empresa tecnológica como paso previo a la auditoría oficial por parte de la entidad certificadora.

3. Estructura de la memoria

En el primer capítulo se ha expuesto la introducción y los objetivos del proyecto.

En el segundo se presentan algunos de los fundamentos de la seguridad informática y lo que representa un SGSI y las bases sobre las que se sustenta.

En el tercer capítulo se abordan los diferentes estándares así como una breve reseña de algunas de las normas internacionales ISO así como normativa nacional.

En el cuarto capítulo se presenta la norma 27001, que es la base de este proyecto y se exponen los cambios que ha sufrido la misma durante su última revisión.

En el quinto capítulo se desarrolla la estructura de documental que debe generar una empresa para poder cumplir con los requerimientos de la norma. También se implementa el documento base en la norma 27001 como es la declaración de aplicabilidad o SOA por sus siglas en inglés. Se ha introducido también un glosario de términos empleados en un SGSI.

Finalmente se presentan las conclusiones, posibles continuaciones del trabajo así como la bibliografía del proyecto.

1. Seguridad de la Información

A primera vista, los términos "Seguridad de la Información" y "Seguridad Informática" pueden parecer lo mismo, más si se parte de la premisa que el desarrollo y la innovación en la tecnología están derivando hacia el formato de "digitalizar" y "gestionar" cualquier tipo de información mediante un sistema informático. No obstante, aunque están destinados a vivir en armonía y trabajar conjuntamente, cada una de las áreas de Seguridad tienen objetivos y actividades diferentes.

La Seguridad Informática (IT Security) se define como la distinción táctica y operacional de la Seguridad, mientras la Seguridad de la Información (Information Security) sería la línea estratégica de la Seguridad.

Partiendo de esta definición de Seguridad Informática, esta rama se encargaría de las implantaciones técnicas de la protección de la información, las implementaciones de software antivirus, cortafuegos, correlación de eventos, detección de intrusos, atención de incidentes, entre otros elementos, que –siguiendo las prácticas de gobierno de tecnología de información- especifican la manera de actuar y como solucionar las situaciones parciales o totales, cuando la información en sí, es el activo que se halla en riesgo.

Por otro lado, la Seguridad de la Información es la disciplina que trata sobre las amenazas, los riesgos, los análisis de escenarios, las buenas prácticas y esquemas normativos, que exigen niveles de aseguramiento de procesos y de tecnologías para subir el nivel de confianza en la creación, uso, transmisión, almacenamiento, recuperación y disposición final de la información.

Entendemos por Seguridad de la Información, como el paquete de medidas preventivas y reactivas de las empresas y de los sistemas tecnológicos que nos permiten resguardar y proteger la información buscando siempre mantener la confidencialidad, la disponibilidad e integridad de la misma.

Para alcanzar ese objetivo, se ayuda en la Seguridad Informática (que como hemos comentado estaría gobernada por las directrices de la Seguridad de la Información), es decir, a pesar de ser materias diferentes, la una no se entiende sin

la otra. De este modo, la Seguridad de la Información se encargará de "regular" y establecer los mecanismos a seguir para la proteger la información.

Es relativamente habitual que la Seguridad de la Información se ayude de una Política de Seguridad desarrollada mediante la creación de un Plan Director de Seguridad. La Dirección (de la empresa) tendrá como labor definir las líneas de actuación (estrategia) en materia de Seguridad y, mediante el Plan Director de Seguridad, determinar las medidas, tanto técnicas como procedimentales, que garanticen los objetivos marcados en la Política de Seguridad.

Las medidas técnicas (tácticas y operativas), serán llevadas a cabo por el personal del equipo de Seguridad Informática, -Administradores/Consultores de Sistemas y Seguridad-, que desarrollarán e implementarán las medidas oportunas para asegurar el cumplimiento de la Política de Seguridad y, además, con el Análisis de Riesgos en el que debe de estar basada la Política.

Podríamos asegurar por lo tanto, que la Seguridad Informática (IT Security) es la parte operacional de la Seguridad, esto es, las medidas técnicas que garantizan la Seguridad de la Información. Basado en (Jeimy J. Cano, 2011) “La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes”

2. Sistema de Gestión de la Seguridad de la Información (SGSI)

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

Entendemos por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, según la norma ISO/IEC 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad (CIA), así como de

los sistemas implicados en su tratamiento, dentro de una organización de todo ese conjunto de datos.

Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados para garantizar su CIA.

Sistema CIA:

- C (Confidentiality - Confidencialidad). La información solamente estará disponible para aquel personal autorizado a su acceso, estando reflejados en el mismo los privilegios específicos (escritura, lectura, modificación, manipulación…) sobre la misma.
- I (Integrity - Integridad). Se deben establecer medios mediante los cuales se pueda verificar y garantizar que la información no ha sido manipulada ni alterada.
- A (Availability - Disponibilidad). Hay que garantizar que la información será accesible por el personal autorizado en el momento necesario, así como su inmediata accesibilidad ante incidentes que directa o indirectamente afecten a la disponibilidad de la misma.

Además, también se encuentran reconocidas las siguientes variables de suma importancia:

- Autenticidad. Comprobar y verificar que los datos tienen como origen el sistema o persona desde donde se dice proviene, ofreciéndonos métodos para la comprobación del emisor y destinatario.
- No repudio. Proveer de medios y herramientas que establezcan la veracidad de la participación de dos partes en una comunicación o intercambio de datos, sin que ninguna de ellas pueda negar la participación, ya que la opuesta posee pruebas irrefutables de la misma.

En base al conocimiento del ciclo de vida de cada información relevante se debe adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

2.1 Algunos conceptos de un SGSI

Para empezar a establecer un SGSI debemos definir los elementos básicos que lo conforman. Estos elementos establecerán las pautas a seguir para realizar una correcta implementación del mismo.

El primer paso para definir un Sistema de Gestión de la Seguridad de la información, es definir, planificar y desarrollar un correcto sistema de evaluación de riesgos. Para ello, hay que establecer el alcance, los objetivos, las estrategias y las políticas.

La línea lógica de acción para este proceso es:

Imagen 1. Proceso SGSI

- Alcance del SGSI

Hay que especificar qué es lo que se quiere proteger y asegurar (departamentos, sistemas, metodologías, procesos, etc...), y será lo que aparezca en el documento de certificación.

Para establecer una matriz inicial de entidades factibles de asegurar indicamos una muestra de ejemplo:

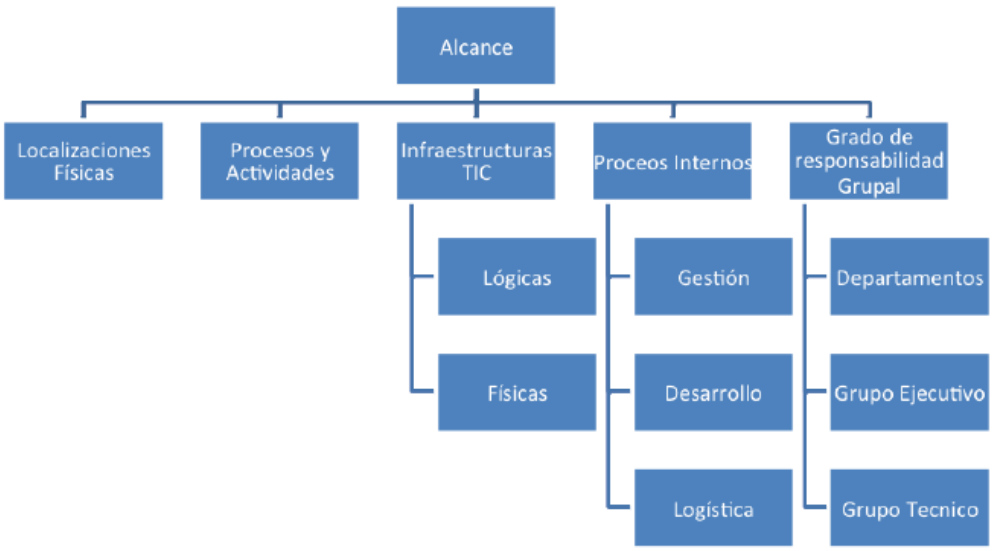


Imagen 2. Matriz de Entidades

Hay que decir que cada uno de los ítems de esta matriz es combinable con uno o varios de la misma. Por ejemplo:

- Asegurar la infraestructura TI global y procesos funcionales del área de gestión en el departamento de ventas.
- Asegurar la infraestructura TI y procesos de la organización para establecer seguridad en los procesos de comunicaciones externas.

- Objetivos y Requerimientos

En esta fase debemos de establecer la situación final que deseamos conseguir y como deben de quedar los procesos para conseguir un estado de seguridad óptimo. Para ello deberemos de tener en cuenta una serie de requerimientos que condicionarán nuestra actuación y metodología y que serán satisfechos con los correspondientes controles:

- Requerimientos:
  - Legalidad y Normativa que afecte de forma directa a la organización
  - Políticas de seguridad internas y normativas internas relativas a la seguridad.
  - Contratos con proveedores, clientes, socios, etc... que condicionen nuestra actuación.
  - Los datos obtenidos del Análisis de riesgos.

Ejemplos de Objetivos y Requerimientos son:

- Establecimiento de los parámetros CIA según la legislación vigente.
- Establecimiento de un plan DLP contra la fuga de información en los departamentos funcionales de ventas y compras.
- Establecimiento de un sistema seguro que mantengan las premisas CIA, para la comunicación del personal externo (agentes).

- Políticas de seguridad

Hay que establecer un sistema de estrategias que nos ayuden a ejecutar los requerimientos y la metodología para llevarlas a cabo.

Las estrategias generadas, crearán políticas de seguridad que irán desde las más globales y, que encuadrarán a grandes operaciones y servicios de la empresa, a todas aquellas generadas para cubrir requerimientos específicos departamentales.

Para ello, podemos definir un sistema jerárquico de políticas de seguridad, como el siguiente:

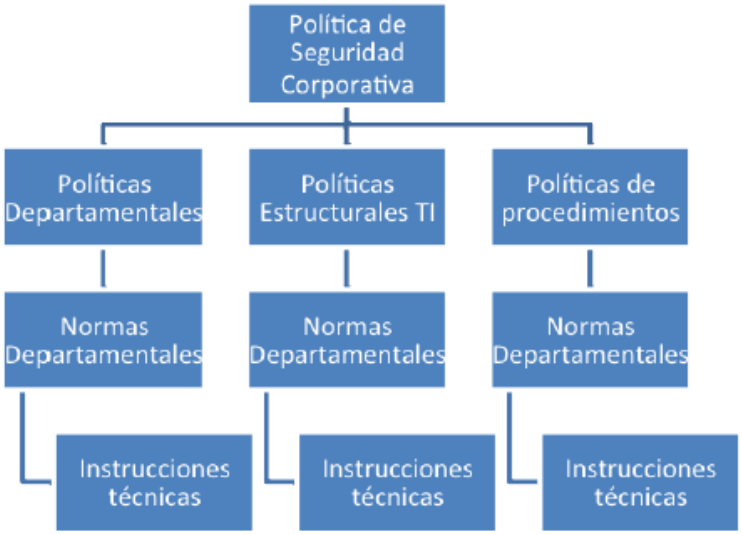


Imagen 3. Sistema jerárquico de políticas de seguridad

Las normas son el desarrollo de la política para un ámbito concreto que necesita especificaciones independientes.

Las instrucciones técnicas son cómo se debe desarrollar la política o norma en un caso específico para su éxito.

2.1.1.- Activos

Según la norma “En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización”.

Matriz de ejemplo de Activos:

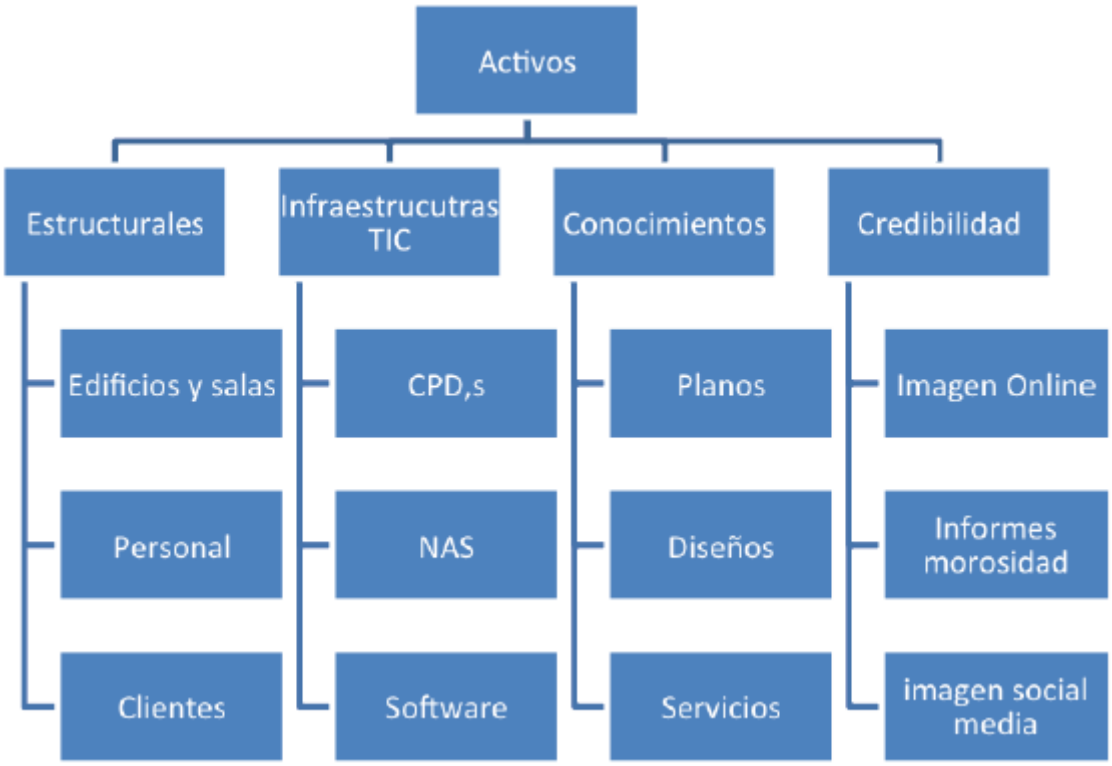


Imagen 4. Matriz de activos

El proceso que se debe de ejercer sobre los mismos es:

- Identificar

  Es esencial identificar los activos más importantes para el proceso de securización.

- Valorar

  Se necesitará analizar cada uno de ellos, así como su implicación en los procesos de la organización y la interoperabilidad con los demás activos, para poder valorarlos de una forma cuantitativa o por su valor funcional en los procesos y su repercusión en CIA.

- Estado de Seguridad

  Establecer el nivel de seguridad que se le aplicará según los datos obtenidos en los anteriores apartados.

2.1.2.- Eventos e Incidentes en la seguridad

La norma define:

- Evento en la Seguridad de la Información

  Ocurrencia detectada en un estado de sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.

- Incidente en la Seguridad de la Información

  Un único evento o una serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones empresariales y de amenazar la seguridad de la información.

Teniendo estos dos conceptos claros, debemos de establecer un sistema para tratar de forma continuada, todos los eventos e incidentes de la seguridad, que ocurren sobre los activos identificados. Estos registros se deben de estructurar para actuar de modo proactivo y evitar que vuelvan a ocurrir.

Para establecer el sistema de gestión de los mismos es necesario contemplar su tratamiento y la acción/reacción ante los mismos.

Ejemplo de tratamiento y de casos:

- **Evento**

  No se puede enviar un email por no recordar la contraseña.
  Se notifica al administrador mediante la apertura de un “ticket” tipo evento.

- **Incidente**

  Nuestro IDS ha detectado un ataque DDoS a la infraestructura de red. Se notifica al responsable mediante la apertura de un “ticket” tipo incidente.

- **Evento**

  El acceso al repositorio de datos ha estado parado durante 1 hora. Se notifica al administrador mediante la apertura de un "ticket" tipo evento.

- **Incidente**

  No se puede recuperar una copia de seguridad de un servidor de producción por no aparecer el responsable que tiene la contraseña. Se notifica al responsable mediante la apertura de un "ticket" tipo incidente.

Podemos definir el ciclo de vida de un incidente como se muestra en el siguiente gráfico:

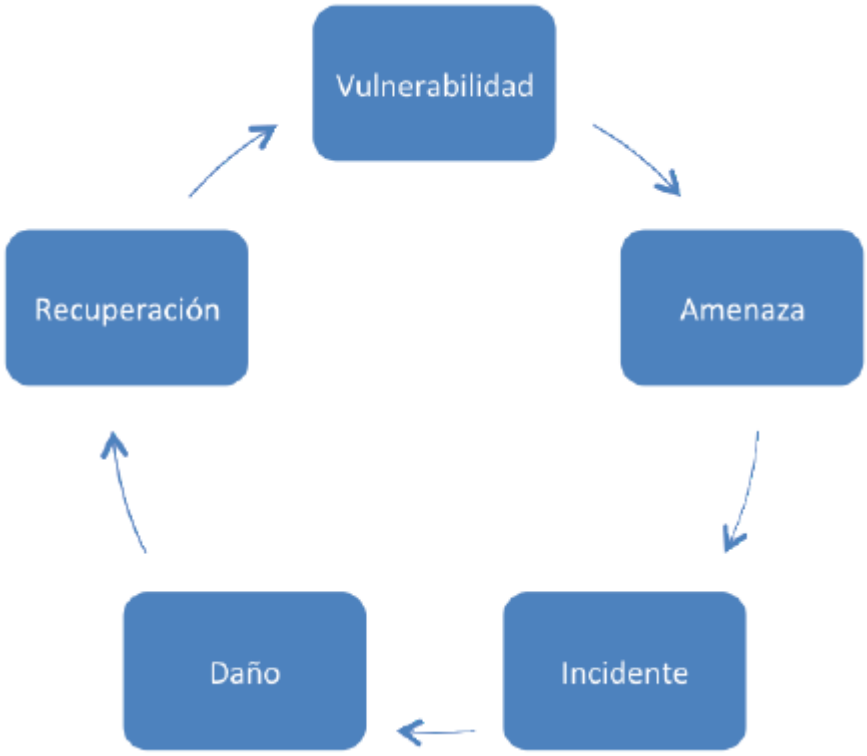


Imagen 5. Ciclo de vida de un incidente

2.1.3.- Amenaza

Según la norma, una amenaza se define como la causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Como podemos observar en el ciclo de vida de un incidente, las amenazas causan incidentes a través de vulnerabilidades, y los incidentes daños en los activos.

El origen de las amenazas puede provenir desde fuentes:

- Humanas intencionadas (Hacking, Robo de información, infección, etc…).
- Humanas no intencionadas (Borrado de información accidental, caída de activo, etc...).
- Medioambientales (Inundaciones, Incendios, terremotos...).
- Accidentales (Descarga eléctrica, parada de la ventilación, etc...).

Se deben de determinar diferentes conceptos de las mismas para poder prevenirnos de ellas y evitar que se puedan convertir en un incidente:

- Procedencia

  Interno o externo, causado por un empleado o por un atacante desde fuera.
- Temporalidad

  Permanente o temporal, temporal sería un ataque contra nuestros servidores, y permanente la destrucción de un activo.
- Tipo de daño (directo o indirecto)

  Directo sería un ataque contra nuestro CPD, e indirecto, una crítica contra la empresa en foros.
- Repercusión

  Se mide la capacidad de hacer daño de la amenaza, y a la cantidad de activos que puede afectar, dándonos un valor de índice de daño.
- Motivación

  Que motiva al atacante a llevar a cabo una amenaza y transformarla en incidente.
- Frecuencia

  Periodicidad de que la amenaza se transforma en incidente, aumentando esto el nivel de criticidad de la misma.

Se pueden englobar en diferentes apartados según su repercusión en CIA:

- Interrupción

  El activo queda inoperativo, no pudiendo ofrecer el servicio o la información, por ejemplo un ataque DoS, o la destrucción de un disco duro. Afecta a: Disponibilidad
- Intercepción

  Un agente sin privilegios accede a un activo o información al que no está autorizado, por ejemplo un atacante que provoca un mitm y lanza un ataque de sniffing. Afecta a: Confidencialidad
- Modificación

  Un agente sin privilegios y sin autorización accede a un activo o recurso y lo modifica, por ejemplo la inclusión de código en un server para lanzar una Shell. Afecta a: Integridad.
- Fabricación

  Un agente diseña y desarrolla objetos no autorizados que realizan acciones en la infraestructura en que perjudican a la seguridad de la misma y de la información. Afecta a: Autenticidad.

3. Gestión de la Información

La seguridad de la información no sólo es una recomendación, sino que se ha establecido como una obligación legal.

Las empresas privadas deben regirse por la Ley Orgánica de protección de Datos (LOPD) y la Administración Pública por el Esquema Nacional de Seguridad (ENS), aunque la LOPD afecta también a las entidades públicas en la parte de datos personales. El ENS solo afecta a la administración pública.

Para poder realizar una correcta implementación y securización de los activos que tengan información, es esencial categorizar la información por nivel de criticidad, y establecer así una escala de alertas.

La información puede ser:

- **Crítica.** Información base para el funcionamiento de la empresa y esencial para su continuidad e integridad.
  Ej: ficheros de clientes y proveedores, diseños industriales de patentes, etc…
- **Valiosa.** Información indispensable para la estructura de la empresa y la cual está supervisada por personal cualificado, si se pone en compromiso la misma puede causar graves daños sobre la estructura corporativa.
  Ej: Información sobre hábitos y características del personal de nuestros proveedores o clientes.
- **Sensible.** Información, que si bien no es crucial para la subsistencia y funcionamiento empresarial, debe de ser supervisada y controlados los accesos a la misma.
  Ej: Listado del personal corporativo y características del mismo.

A continuación, se van a definir ciertos conceptos que se van a tratar al hablar de seguridad de la información:

- Activo. Un activo es cualquier bien que tiene valor para la organización
- Vulnerabilidad**.** Se denomina vulnerabilidad a la característica de un activo que puede conllevar una debilidad en el mismo y, por lo tanto, comprometerlo**.**
- Amenazas**.** Se catalogan como amenazas al personal y los medios, tanto físicos como lógicos, que pueden aprovechar la/las vulnerabilidades de un activo**.**
- Riesgo**.** Se categoriza como riesgo a la probabilidad que una amenaza ponga en compromiso un activo mediante una vulnerabilidad.
- Seguridad**.** Se entiende como Seguridad a las salvaguardas y medidas preventivas y reactivas que se utilizan para paliar o evitar las vulnerabilidades y amenazas y, por lo tanto, disminuir el riesgo**.**

El primer paso para establecer un Sistema de Gestión de Seguridad es realizar un inventario de todos los activos y la información que contienen, con la criticidad asociada a cada una de ellas.

La seguridad de la información es aplicable en todo el ciclo de vida de la información:

- Asegurando el canal desde donde recibimos los datos (si es factible)
- Asegurando el medio donde recibimos los datos.
- Asegurando el aplicativo donde se va a consultar y tratar la misma
- Asegurando el medio por el cual se va a compartir con el resto de usuarios.
- Asegurando el sistema CIA con respecto a la misma.
- Asegurando la transferencia a terceros.
- Asegurando los medios alternativos de difusión o consulta, como puede ser la impresión física.

Como se ha comentado anteriormente, debido a la gran difusión e intercomunicación entre todos los sistemas, es necesario que los datos sean accesibles desde múltiples orígenes, local, internet, intranet, etc…Este escenario hace que las amenazas sean cada vez más crecientes.

Ya se han visto las amenazas que pueden afectar a nuestros activos, pero no sólo están las que provienen de software o de la falta de experiencia del administrador con respecto la seguridad de los sistemas que controla, sino las que provienen del hardware o de elementos externos (corriente eléctrica, malfuncionamiento del hardware, cambio de proveedor externo TIC, etc…).

Dado que los medios técnicos no cubren, en su gran mayoría, todas las necesidades de seguridad global, es necesario establecer un sistema de procedimientos, controles y planificación de políticas y planes de acción/reacción.

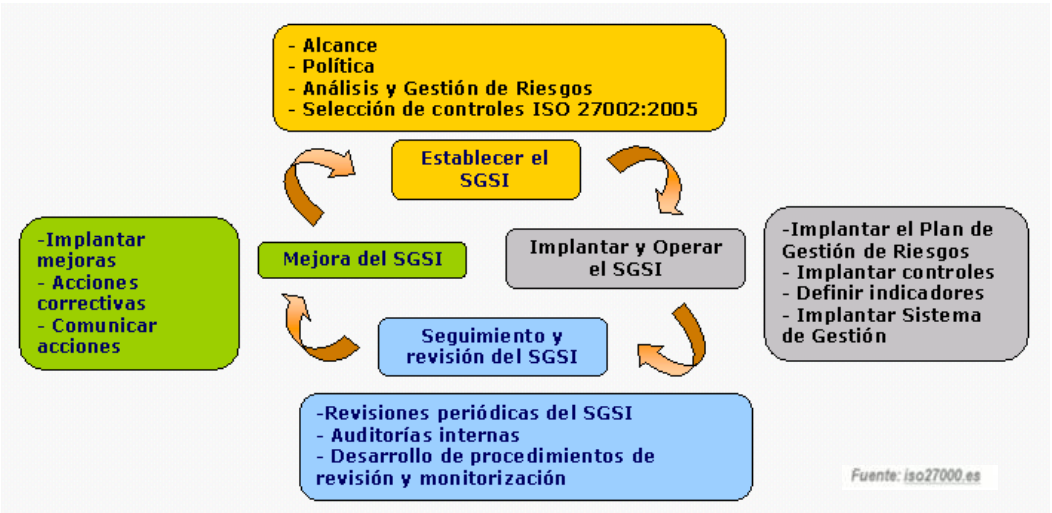


Imagen 6. Proceso SGSI

3.1 Ciclo de Vida de la Seguridad de la Información

En base al conocimiento del ciclo de vida de cada información relevante se debe adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

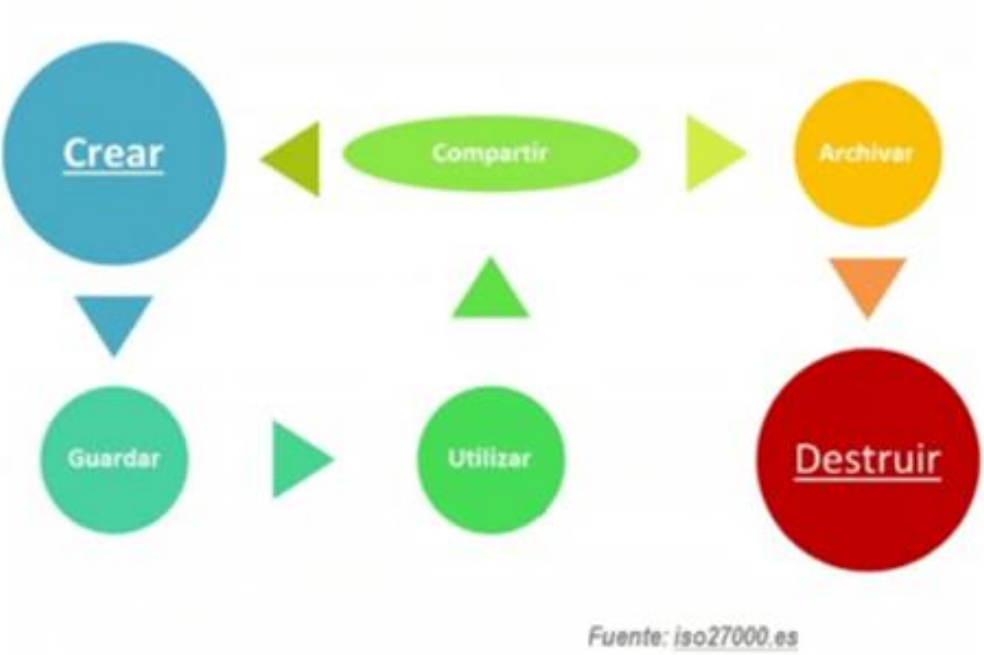


Imagen 7. Ciclo de vida de la información

1. Definiciones

1.1 Normas

Las normas (dentro de este contexto ISO y UNE) no son obligatorias, es opcional que una empresa las acate o no, pero debido a la excelencia y la fiabilidad que ofrecen, por ejemplo un cliente que interactúe con la misma, asume que su proveedor sigue unos protocolos y que ofrece unas garantías mínimas que se basan en la norma.

1.2 Estándares

CNCIE nos ofrece un párrafo que identifica perfectamente un estándar y su cometido:

El diccionario de la Real Academia de la Lengua dice que un estándar es lo "que sirve como tipo, modelo, norma, patrón o referencia". En el campo técnico la estandarización es el proceso por el cual se establecen unas normas comúnmente aceptadas que permiten la cooperación de diferentes empresas o instituciones sin menoscabar su posibilidad de competir. Un estándar proporciona ventajas no sólo a las empresas, sino también al usuario, ya que así no ve limitada su capacidad de elección a un determinado proveedor, sino a todos aquellos que cumplen un estándar determinado y que, por tanto, crean productos que son compatibles.

Hay varios tipos de estándares:

- Para la administración
- Para el sistema de gestión
- Para los procesos
- Para la evaluación
- Para los productos

Los principales organismos internacionales desarrolladores de estándares para telecomunicaciones, son:

- ETSI - European Telecommunications Standards Institute (Instituto Europeo de Estándares de Telecomunicaciones)
- IEC - International Electrotechnical Commission (Comisión Electrotécnica Internacional)

- IEEE - Institute of Electrical and Electronical Engineers (Instituto de Ingenieros Eléctricos y Electrónicos)
- ISO - Organización Internacional para la Estandarización
- ITU/UIT - Unión Internacional de Telecomunicaciones

Como preámbulo a la descripción de las diferentes normas que se van a desarrollar, se van a introducir brevemente ciertos conceptos sobre el ENS (Esquema Nacional de Seguridad), ya que se ha considerado muy interesante tomar como referencia los principios de seguridad que utiliza el ENS al ser un Real Decreto que regula la utilización de la tecnología y su seguridad por la administración pública, aunque no se trate de una norma al uso.

2. Esquema Nacional de Seguridad

- **Artículo 4. Principios básicos del ENS**

El objeto último de la seguridad de la información es asegurar que una organización administrativa podrá cumplir sus objetivos utilizando sistemas de información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

a) Seguridad integral.

b) Gestión de riesgos.

c) Prevención, reacción y recuperación.

d) Líneas de defensa.

e) Reevaluación periódica.

f) Función diferenciada.

- **Artículo 5. La seguridad como un proceso integral**

1. La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

2. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

- **Artículo 6. Gestión de la seguridad basada en los riesgos**

1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.

2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

- **Artículo 7. Prevención, reacción y recuperación**

1. La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.

2. Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición.

3. Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo.

4. Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.

5. Sin merma de los demás principios básicos y requisitos mínimos establecidos, el sistema garantizará la conservación de los datos e informaciones en soporte electrónico. De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

- **Artículo 8. Líneas de defensa**

1. El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita:

a) Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.

b) Reducir la probabilidad de que el sistema sea comprometido en su conjunto.

c) Minimizar el impacto final sobre el mismo.

2. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

- **Artículo 9. Reevaluación periódica**

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

- **Artículo 10. La seguridad como función diferenciada**

En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.

El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

Como se puede observar, estos principios no sólo pueden cubrir las necesidades de una administración pública, sino de cualquier empresa u organización.

A grandes rasgos un buen procedimiento lógico para implementar las medidas de seguridad apropiadas y mantenerlas, puede ser el siguiente:

- Identificar los activos y necesidades
    - Evaluación de Riesgos
        - Identificación de Amenazas
        - Evaluación de Vulnerabilidades
        - Probabilidad de Ocurrencia
        - Impacto potencial
    - Requisitos legales y normativos de obligado cumplimiento por la organización y empresas que interaccionen con ella
- Identificar riesgo, vulnerabilidades, amenazas
- Establecer medidas tecnológicas, políticas y procedimientos para mitigar el riesgo
- Establecer un sistema de autoaprendizaje ante los incidentes de seguridad, con una retroalimentación activa y un sistema de reacción y mitigación

3. Serie de normas 27000

La serie de normas ISO/IEC 27000 son un conjunto de estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). Los rangos de numeración reservados por ISO van desde el 27000 al 27019 y del 27030 al 27044. La más influyente es la 27001, siendo las demás, especificaciones de partes concretas en torno a la seguridad informática.

Basado en " (iso27001.es, s.f.)".

- **ISO/IEC 27000**

  ISO/IEC 27000 es un conjunto de estándares creados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de

gestión de la seguridad de la información utilizable por cualquier tipo de empresa, pública o privada, grande o pequeña.

Un poco de historia:

Desde 1901 y, como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes normas como:

- BS 5750. Publicada en 1979. Origen de ISO 9001
- BS 7750. Publicada en 1992. Origen de ISO 14001 - BS 8800. Publicada en 1996. Origen de OHSAS 18001 La norma BS 7799 de BSI apareció por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) se elaboró como una guía de buenas prácticas, para la que no se establecía un esquema de certificación. Es la segunda parte (BS 7799-2), publicada en 1998, se establecieron los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente (como por ejemplo AENOR).
Las dos partes de la norma BS 7799, se revisaron en 1999 y la primera parte se adoptó por ISO, sin grandes cambios, como ISO 17799 en el año 2000.
En 2002, se actualizó la segunda parte (BS 7799-2), para adecuarse a la filosofía de las normas ISO de sistemas de gestión.
En 2005, con más de 1700 empresas certificadas en BS 7799-2, esta norma se publicó por ISO, como estándar ISO 27001. Al tiempo, se revisó y se actualizó la ISO 17799. Esta última norma se renombró como ISO 27002:2005 el 1 de julio de 2007, manteniendo el contenido como el año de publicación formal de la revisión.
En marzo de 2006, posteriormente a la publicación de ISO 27001:2005, BSI publicó la BS 7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.
Asimismo, ISO ha continuado (y continúa aún) desarrollando otras normas dentro de la serie 27000 que sirvan de apoyo a las organizaciones en la

interpretación e implementación de ISO/IEC 27001, que es la norma principal y única certificable dentro de la serie.

- **ISO/IEC 27001**

  Publicada el 15 de octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican, por auditores externos, los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Desde el 28 de Noviembre de 2007, esta norma está publicada en España como UNE-ISO/IEC 27001:2007. Ha sido revisado extensamente en 2013, alineándola con las otras normas de sistemas de gestión ISO certificada. Más adelante desarrollaremos esta norma con más profundidad.

- **ISO/IEC 27002**

  Desde el 1 de julio del 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de creación. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. La norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005. Publicada en España como UNE-ISO/IEC 27002:2009 desde el 9 de Diciembre de 2009. Al igual que la anterior, se ha publicado una nueva versión ISO 27002:2013 que contiene 114 controles por los 133 de la versión de 2005. Estos controles se han dividido en 14 dominios añadiendo granularidad a los 11 de 2005.

- **ISO/IEC 27003**

  Publicada el 01 de febrero de 2010. No es certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo con ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación. En España esta norma aún no está traducida.

- **ISO/IEC 27004**

  Publicada el 7 de diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001. En España esta norma aún no está traducida.

- **ISO/IEC 27005**

  Publicada el 4 de junio de 2008 y en una segunda edición en junio de 2011. No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos, sin embargo no provee ningún método específico para la gestión de riesgos de la seguridad de la información. Su publicación revisa y retira las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000. En España esta norma aún no está traducida.

- **ISO/IEC 27006**

  Publicada el 1 de marzo de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para

las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

- **ISO/IEC 27007**

  Publicada en noviembre de 2011. Proporciona una guía para las entidades certificadoras, auditores internos y externos que auditan SGSI contra la norma ISO / IEC 27001. ISO / IEC 27007 se refiere en gran medida a la norma ISO 19011, el estándar ISO para los sistemas de gestión de calidad de auditoría y gestión medioambiental. Se basa también en la norma ISO 17021 Evaluación de la conformidad - Requisitos para los organismos que realizan la auditoría y certificación de sistemas de gestión y se alinea con la norma ISO / IEC 27006, que como hemos visto anteriormente es la norma de acreditación para organismos de certificación del SGSI.

- **ISO/IEC 27008**

  Publicada en noviembre de 2011. Esta norma proporciona una guía para todos los auditores de cuentas sobre los controles en el SGSI seleccionados a través de un enfoque basado en el riesgo (como se presenta en una declaración de aplicabilidad) para la gestión de seguridad de la información. Es compatible con el proceso de información de seguridad de la gestión del riesgo y auditorías internas, externas y de terceros de un SGSI para explicar la relación entre el SGSI y sus controles. Proporciona también orientación sobre la manera de verificar la medición que requieren los controles de SGSI que se implementan. Además, es compatible con cualquier organización que utilice la norma ISO / IEC 27001 y la ISO / IEC 27002 para satisfacer los requisitos de garantía y como plataforma estratégica para el gobierno de la seguridad de la información.

- **ISO/IEC 27010:**

  Fue publicada en abril 2012. Es una norma dividida en 2 partes, que consiste en una guía para la gestión de la seguridad de la información en relación con el intercambio de información sobre los riesgos de seguridad de la

información, los controles, los problemas y/o incidentes que abarcan los límites entre sectores de la industria y/o naciones, en particular los que afectan a la "infraestructura crítica".

- **ISO/IEC 27011**

  Publicada en diciembre de 2008. Es una guía para la implementación y gestión de la seguridad de la información en organizaciones del sector de las telecomunicaciones basada en ISO/IEC 27002. Está publicada también como norma ITU-T X.1051. La norma está siendo revisada para adecuarla a las nuevas versiones de la norma ISO / IEC 27001 y 27002. En España, aún no está traducida.

- **ISO/IEC 27013**

  Publicada en octubre de 2012. Consiste en una guía de implementación integrada de las normas ISO/IEC 27001 (gestión de seguridad de la información) e ISO/IEC 20000-1 (gestión de servicios TI).

- **ISO/IEC 27014**

  Publicada en 2013 como ISO/IEC 27014 y ITU-T X.1054. La norma proporciona una guía sobre los conceptos y principios del Gobierno de la Seguridad de la Información, mediante el cual las organizaciones pueden evaluar, dirigir, supervisar y comunicar las actividades relacionadas con la Seguridad de la Información dentro de la propia organización y es aplicable a todos los tipos y tamaños de organizaciones.

- **ISO/IEC 27015**

  Fue publicada en 2012. Consiste en una guía para organizaciones del sector financiero y de seguros (bancos, compañías de seguros, compañías de tarjetas de crédito, etc.) que les permite implementar un SGSI usando los estándares ISO27000.

- **ISO/IEC 27016**

  La norma fue publicada en 2014 como Informe Técnico en lugar de una norma internacional completa. Este Informe Técnico proporciona directrices sobre la economía en la seguridad de la información como un proceso de

toma de decisiones en relación con la producción, distribución y consumo de bienes y servicios, cada una de las cuales tienen usos alternativos con el fin de lograr las metas de una organización con un costo mínimo.

- **ISO/IEC 27017**

  Esta norma proporciona una guía sobre los elementos de seguridad de la información de la computación en nube, para recomendar y asistir en la aplicación de los controles de seguridad de la información en la nube que complementa la orientación en la norma ISO / IEC 27002 y otras normas de la familia ISO2700 incluyendo ISO / IEC 27018 en los aspectos de privacidad de la computación en nube, la norma ISO / IEC 27031 en la continuidad del negocio, y la norma ISO / IEC 27036-4 sobre la gestión de la relación.

- **ISO/IEC 27018**

  Esta norma proporciona una guía destinada a garantizar que los proveedores de servicios en la nube (como Amazon y Google) ofrezcan controles adecuados sobre la seguridad de la información para proteger la privacidad de los clientes asegurando PII (Información de Identificación Personal).
  La norma será seguida por la norma ISO / IEC 27017 y cubre los ángulos de seguridad de la información más amplios de la computación en la nube, con excepción de la privacidad. La norma fue publicada en agosto de 2014.

- **ISO/IEC 27019**

  Esta norma (Informe Técnico) está destinada a ayudar a las organizaciones de la industria de la energía a interpretar y aplicar la norma ISO / IEC 27002 con el fin de asegurar sus sistemas de control de procesos electrónicos. La norma fue publicada en 2013.

- **ISO/IEC 27031**

  Consiste en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones. El estándar sugiere una estructura o marco (en realidad un conjunto de métodos y procesos) para cualquier organización ya sea privada, gubernamental o no gubernamental. Identifica y especifica todos los aspectos pertinentes, incluidos los criterios de rendimiento, diseño y detalles de implementación, para mejorar la preparación de las TIC como

parte del SGSI de la organización, ayudando a asegurar la continuidad del negocio. Fue publicada en 2011.

- **ISO/IEC 27032**

  Oficialmente, la norma ISO / IEC 27032 "ciberseguridad" o "seguridad en el Ciberespacio", es definida como la "preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio". A su vez el "ciberespacio" (definido completamente en la norma) se define como "el entorno complejo que resulta de la interacción de las personas, software y servicios a través de Internet por medio de dispositivos y redes conectados a él, que no existe en ninguna forma física. En la práctica, la norma trata sobre la seguridad en Internet. Fue publicada en el 2011.

- **ISO/IEC 27033**

  Norma dedicada a la seguridad en redes, dividida en 7 partes: 27033-1, conceptos generales (publicada en diciembre de 2009); 27033-2, directrices de diseño e implementación de seguridad en redes (2011); 27033-3, escenarios de redes de referencia (2011); 27033-4, aseguramiento de las comunicaciones entre redes mediante gateways de seguridad (2012); 27033-5, aseguramiento de comunicaciones mediante VPNs (2012); 27033-6, convergencia IP (2012); 27033-7, redes inalámbricas (2012). El propósito de la norma es proporcionar una guía detallada sobre los aspectos de seguridad de la gestión, el funcionamiento y el uso de redes en sistemas de información y sus interconexiones.

- **ISO/IEC 27034**

  Consiste en una guía de seguridad en aplicaciones informáticas. Al igual que el anterior, este estándar se divide en varias partes (7) y proporciona una guía sobre la especificación, diseño / selección y la aplicación de controles de seguridad de la información a través de un conjunto de procesos integrados a través del Ciclo de Vida de Desarrollo de Sistemas de una organización/es (SDLC). Fue publicada en 2011.

- **ISO/IEC 27035**

  La norma abarca los procesos de gestión de seguridad de la información de eventos, incidentes y vulnerabilidades. Se apoya en la norma 27002 para la gestión de incidentes de seguridad de la información. Fue publicada en 2011 y se prevé una actualización en 2016.

- **ISO/IEC 27036**

  Consiste en una guía de seguridad de los procesos de outsourcing (externalización de servicios). Este estándar ofrece una guía sobre la evaluación y el tratamiento de los riesgos de seguridad de información que intervienen en la adquisición de bienes y servicios con los proveedores. Está dividida en 4 partes. Fue publicada en 2012.

- **ISO/IEC 27037**

  Esta norma proporciona una guía sobre la identificación, recolección/recepción, adquisición, manejo y protección/preservación de pruebas forenses digitales es decir, "los datos digitales que pueden ser de valor probatorio" para su uso en los tribunales. Fue publicada en 2012.

- **ISO/IEC 27038**

  La norma específica las características técnicas para la redacción de documentación digital. Fue publicada en 2014.

- **ISO 27799**

  Publicada en junio de 2008. Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de la norma ISO/IEC 27002, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes.

4. Norma ISO 27001

Son válidas estas dos formas de nombrar a la norma:

- UNE-ISO/IEC 27001:2014 (UNE=Una norma Española / :2014 = fecha de creación).
- ISO/IEC 27001:2013 (como se ve, AENOR adaptó la norma al ámbito nacional al año de aparecer).

La norma ISO 27001 persigue conseguir establecer de forma eficiente los requerimientos de seguridad CIA, y diseñar una metodología de gestión de la seguridad de la información, denominada SGSI (Sistema de Gestión de la Seguridad de la información) ó ISMS (Information Security Management System), como ya hemos explicado anteriormente.

Elaborada por UNE ISO/IEC 27001 y traducida al español por AENOR forma parte de la serie de normas 27000. La publicación ISO/IEC 27001:2013 atiende al nuevo esquema definido por ISO para los sistemas de gestión acorde al formato denominado “Anexo SL” de 10 cláusulas, ya aplicado inicialmente en estándares como ISO/IEC 22301 y que será de próxima aplicación a revisiones de estándares relevantes como ISO/IEC 9001:2015, ISO/IEC 14001:2015, entre otros. Este marco común, procede de la Guía 83 de ISO y mejora sustancialmente la capacidad de integración de varios sistemas de gestión independientemente de los estándares de referencia.

ISO/IEC 27001 se divide en 11 secciones más el anexo A; las secciones 0 a 3 son introductorias (y no son obligatorias para la implementación), mientras que las secciones 4 a 10 son obligatorias, lo que implica que una organización debe implementar todos sus requerimientos si quiere cumplir con la norma. Los controles del Anexo A deben implementarse sólo si se determina que corresponden en la Declaración de aplicabilidad.

De acuerdo con el “Anexo SL” de las Directivas ISO/IEC de la Organización Internacional para la Normalización, los títulos de las secciones de ISO 27001 son los mismos que en ISO 22301:2012, en la nueva ISO 9001:2015 y en otras normas de gestión, lo que permite integrar más fácilmente estas normas.

A continuación, describimos brevemente las diferentes secciones de UNE-ISO/IEC 27001:2014 (Leal, 2015):

- **Sección 0 – Introducción –** detalla el objetivo de ISO 27001 y su interoperabilidad con otras normas de gestión.

- **Sección 1 – Alcance –** informa que esta norma es aplicable a cualquier tipo de organización.
- **Sección 2 – Referencias normativas –**referencia a la norma ISO/IEC 27000 como el estándar en el que se proporcionan términos y definiciones.
- **Sección 3 – Términos y definiciones –** de nuevo, hace referencia a la norma ISO/IEC 27000.
- **Sección 4 – Contexto de la organización –** esta sección, define los requerimientos para comprender cuestiones externas e internas, también especifica las partes interesadas, sus requisitos y el alcance del SGSI.
- **Sección 5 – Liderazgo –** en esta sección se definen las responsabilidades de la dirección, el establecimiento de roles y el contenido de la política de alto nivel sobre seguridad de la información.
- **Sección 6 – Planificación –** esta sección define los requerimientos para la evaluación y el tratamiento de riesgos, la declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.
- **Sección 7 – Apoyo –** esta sección detalla los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.
- **Sección 8 – Funcionamiento –** esta sección define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.
- **Sección 9 – Evaluación del desempeño –** esta sección define los requerimientos para la monitorización, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.
- **Sección 10 – Mejora –** esta sección define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.
- **Anexo A –** este anexo proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 secciones (secciones A.5 a A.18).

Todas las normas de calidad y, por supuesto, la 27001, orientan su base en los procesos. Un proceso es toda aquella actividad que mediante una entrada (información, datos, materiales, etc…) desarrolla una salida (documentos, bbdd, producto, etc…).

Mediante el desarrollo de una matriz de procesos se podría establecer la dinámica de una organización y sus flujos, tanto internos como externos.

El SGSI es, en sí, un proceso que recibe como entradas una serie de requerimientos dada una serie de activos (físicos, lógicos, procesos, personas, etc…) y, mediante una transformación, ofrece una salida que nos da el estado de seguridad del propio activo.

El proceso o procesos que realiza el SGSI para la transformación de los activos, siguen una estructura denominada PDCA (o en castellano PHVA). Aunque en la nueva versión de la norma, no se hace tan evidente la estructuración del contenido siguiendo este estándar de facto, este modelo sigue estando muy presente. De hecho, hemos dedicado el Anexo 1 para explicar en detalle el denominado Ciclo de Deming.

- **Plan -> Planificar**

  Estudiar los Objetivos, Requerimientos, Políticas y procedimientos que debe seguir el SGSI, para obtener el resultado requerido. Es en este punto donde se origina el SGSI y toda la documentación relacionada (registros, informes iniciales, etc…).

- **Do -> Hacer**

  Implementar en la infraestructura empresarial las medidas, procedimientos, controles, políticas y procesos que doten de seguridad a los activos objetivo.

- **Check -> Verificar**

  Fijar unos controles que informen de la efectividad del proceso de implementación y reportar dichos datos para la revisión. En este punto se

valorará la eficiencia del SGSI y sus resultados en auditorías internas revisadas por el auditor.

- **Act -> Actuar**

  Diseñar acciones y revisiones de las medidas adoptadas según las verificaciones obtenidas, para establecer los cambios apropiados y conseguir así el objetivo. Se fijarán las acciones preventivas y correctivas necesarias, así como se mejorará el estado del SGSI.

Como ya hemos comentado anteriormente, la ISO 27001 es la única certificable de todo el conjunto de estándares de la familia 27000, su implementación y seguimiento no es obligatorio, únicamente es recomendable, pero una vez establecido, se puede certificar por aquellas organizaciones autorizadas (AENOR, SGS, BSI, etc…) a tal cometido, lo cual ofrecería el reconocimiento certificado a nivel internacional del seguimiento y éxito en la implementación de la seguridad de la información en el alcance detallado y esto es importante ya que se certificará el ámbito que se haya marcado, ya que muchas empresas solamente certifican ciertos departamentos (o procesos) y no toda la base empresarial. De hecho y, basándome en mi experiencia, es la práctica habitual.

4.1 Cambios en la versión 2013

Quizás la mayor diferencia entre la anterior y la nueva norma es su estructura. ISO/IEC 27001:2005 estaba dividida en cinco secciones principales (4 a 8) y ISO/IEC 27001:2013 tiene siete (4 a 10). Esto es debido (como hemos comentado anteriormente), a que la nueva edición 2013 utiliza el formato acordado por ISO para todas sus normas, el Anexo SL.

En general, la nueva norma parece más focalizada que la anterior. Una prueba de ello es que, aunque tiene más secciones (siete frente a cinco), éstas son aproximadamente un 25% más cortas, (excluidos los anexos). Esto debería hacer que sea más fácil realizar la implantación de la norma en una corporación, aunque seguramente no todas las empresas piensen de la misma manera.

La nueva norma no se centra en el proceso (aunque todavía se habla de ellos) y, como se mencionó en el punto 4, no está diseñada basándose en el modelo PDCA. La versión de 2005 tenía toda una subsección enfocada al proceso, sin embargo, el nuevo estándar lo pasa por alto ya que ISO reconoce que el requisito realmente importante es la mejora continua y, por lo tanto, existen otras formas, además del PDCA, igualmente válidas para cumplir este requisito. (Borghello, Más cambios en la ISO 27000:2013, 2013)

La gestión de acciones preventivas también ha desaparecido. Las empresas que decidieron establecer el estándar 27001 en sus organizaciones con la versión anterior, comenzaban a realizar la gestión de riesgos en base al tratamiento del propio riesgo y esto no era del todo práctico, ya que la gestión de riesgos ya está enfocada hacia la prevención de posibles problemas y por lo tanto, no hay necesidad de especificar una clausula separada con la acción preventiva. Una vez que se inician las técnicas de gestión de riesgos, la acción preventiva es redundante.

También es importante indicar que nace un nuevo término: "el dueño de riesgo" (*risk owners*), por lo que el nivel de responsabilidad es empujado hacia arriba, a un nivel más alto. (Borghello, 2013)

En la nueva norma también se ha eliminado la distinción entre documentos y registros. Ahora toda la documentación se denomina "información documentada".

Por el contrario, aparece un nuevo concepto llamado contexto. Lo que se pretende en el nuevo estándar es que se llegue a conocer realmente el contexto de su organización antes de establecer un SGSI. Esto significa que se deben de entender las necesidades y expectativas de las partes interesadas, el enfoque de la dirección, su cultura, sus capacidades, sus obligaciones legales y su sistema político, económico, tecnológico y medioambiental. Una vez contextualizado todo esto, será mucho más sencillo definir el alcance de su SGSI y acometer los retos a los que se debe hacer frente antes de implantar la nueva norma.

Otro reseña importante que tiene que ver con lo expresado en el punto anterior es que en el punto 4.1 de la norma, hace referencia a la norma ISO 31000:2009 para determinar la gestión de riesgos estándar en base al contexto interno y externo de la organización. De hecho, esto es el punto neurálgico de la nueva norma. Esta mención de la norma ISO 31000, no es casualidad, ya que se podría decir, que se ha tomado esta norma como punto de partida para realizar la nueva versión, o al menos conceptualmente, ya que se pretende que se utilice la noción que define la ISO 31000 de riesgo y, con ese enfoque, se realice la evaluación de riesgos y el posterior tratamiento de los mismos (punto 6.1.3). Esto ayudará a asegurar que las organizaciones que desarrollan sus sistemas de gestión de seguridad de información lo dirijan hacia sus propias necesidades y requisitos, lo que puede suponer un auténtico reto en algunas organizaciones.

Sin embargo, no todos los aspectos de la nueva norma son tan drásticos. El Anexo A es ahora más fácil de usar. Aunque en la nueva norma todavía se enumeran los controles y los objetivos de control, se pueden ignorar estos últimos si se desea hacerlo. El nuevo estándar únicamente establece en su punto 6.1.3.d) "*elaborar una "Declaración de Aplicabilidad" que contenga los controles necesarios".* No hay mención sobre los objetivos de control. De hecho, en la nota 2 de su punto c), indica que *"Los objetivos de control se incluyen implícitamente en los controles seleccionados".*
(Limited, 2014)

En el siguiente cuadro, se puede ver como se ha estructurado la nueva norma comparándola con la antigua:

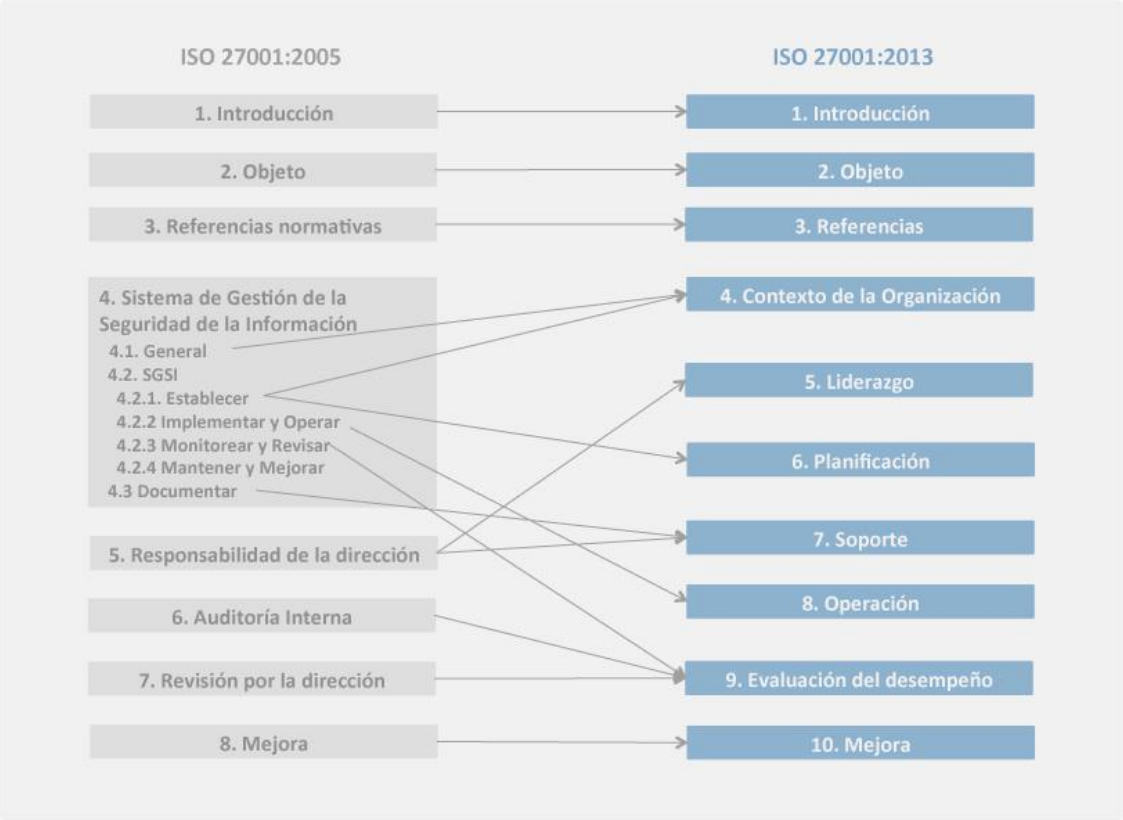


Imagen 8. Cambios versión 2014. (Excellence, 2014)

Otro cambio en la nueva norma, es que los Anexo B y C han desaparecido. El Anexo A, sigue formando parte del texto de la norma con la enumeración de los controles. Más adelante detallamos todos los cambios que ha sufrido esta parte de la norma.

En la siguiente tabla, se comparan las cláusulas de la nueva norma con respecto a la anterior versión (García, 2013):

Cláusula ISO 27001:2005	Cláusula ISO 27001:2013	Observaciones
0 Introducción 1.1 General 1.2 Enfoque de procesos 1.3 Compatibilidad con otros sistemas de gestión	**0 Introducción**	Las secciones de enfoque a procesos y la compatibilidad con otros estándares ISO, viene de la alineación al Anexo SL de las Directivas de ISO/ IEC Parte 1 y ya no al ciclo PDCA.
1 Alcance 1.1 General 1.2 Aplicación	**1 Alcance**	En la nueva versión es obligatorio cumplir con las cláusulas 4 a la 10 para poder certificarse.

2 Referencias normativas	**2 Referencias Normativas**	Ahora hace referencia a la ISO 27000
3 Términos y definiciones	**3 Términos y definiciones**	Se han excluido todos los términos y definiciones, quedando referenciados a la ISO 27000
4 Sistema de gestión de seguridad de la información 4.1 Requerimientos generales 4.2 Establecimiento y gestión del SGSI 4.2.1 Establecer el SGSI 4.2.2 Implementar y operar el SGSI 4.2.3 Monitorear y revisar el SGSI 4.2.4 Mantener y mejorar el SGSI 4.3 Requerimientos documentales 4.3.1 General 4.3.2 Control de documentos 4.3.3 Control de registros	**4 Contexto de la organización** 4.1 Entendiendo la organización y su contexto 4.2 Entendiendo las necesidades y expectativas de las partes interesadas 4.3 Determinando el alcance del sistema de gestión de seguridad de la información 4.4 Sistema de gestión de seguridad de la información	Una vez que se entiende la organización (contexto) y las necesidades de las partes interesadas, se puede establecer el alcance del SGSI.
5 Responsabilidades de la dirección 5.1 Compromiso de la dirección 5.2 Gestión de recursos 5.2.1 Provisión de recursos 5.2.2 Capacitación, concientización y competencia	**5 Liderazgo** 5.1 Liderazgo y compromiso 5.2 Política 5.3 Roles organizacionales, responsabilidades y autoridades	Se introduce el término “alta dirección” (top management) quien debe demostrar liderazgo y compromiso sobre el SGSI. Adicionalmente a establecer la política ahora, es un requisito obligatorio establecer objetivos de seguridad.

Tabla 1. Cláusulas ISO 27001

Sobre el Anexo A (ISO 27002), estos son los cambios producidos por la nueva reestructuración (García, 2013):

Anexo A ISO 27001:2005	Anexo A ISO 27001:2013
A.5 Política de Seguridad	A.5 Políticas de Seguridad
A.6 Organización de seguridad de la información	A.6 Organización de la seguridad de la información
A.8 Seguridad en recursos humanos	A.7 Seguridad en recursos humanos
A.7 Administración de activos	A.8 Administración de activos
A.11 Control de acceso	A.9 Control de acceso
	A.10 Criptografía
A.9 Seguridad física y ambiental	A.11 Seguridad física y ambiental
A.10 Administración de comunicaciones y operaciones	A.12 Seguridad en operaciones
	A.13 Seguridad en comunicaciones
A.12 Adquisición, desarrollo y mantenimiento de sistemas	A.14 Adquisición, desarrollo y mantenimiento de sistemas
	A.15 Relación con proveedores
A.13 Administración de incidentes de seguridad de la información	A.16 Administración de incidentes de seguridad de la información
A.14 Administración de continuidad del negocio	A.17 Aspectos de seguridad de la información en la administración de continuidad del negocio
A.15 Cumplimiento	A.18 Cumplimiento

Tabla 2. Cambios Anexo A

Se añade a continuación una lista con los controles que se han eliminado en la nueva versión (Trejo, ISO-27001:2013 ¿Qué hay de nuevo?, 2013):

Control	Descripción	Cambia por	Incluye los controles de la ISO 27001:2005
A.6.1.1	Comité de gestión para la seguridad de la información	Roles de la seguridad de la información y sus responsabilidades	A.6.1.3 y A.8.1.1
A.6.1.2	Coordinación de seguridad de la información	Contacto con autoridades	A.6.1.6
A.6.1.4	Procesos de autorización para instalaciones para procesamiento de información	Seguridad de la información en la gestión de proyectos	
A.6.2.1	Identificación de riesgos relacionados con agentes externos	Política de dispositivo móvil	A.11.7.1
A.6.2.2	Direccionamiento de seguridad al tratar con clientes	Trabajo a distancia	A.11.7.2
A.10.2.1	Entrega del servicio		
A.10.7.4	Seguridad del sistema de documentos		
A.10.8.5	Sistema de información de negocios		
A.10.10.2	Seguimiento al uso de sistema		

A.10.10.5	Falla en el registro		
A.11.4.2	Autenticación de usuarios para conexiones externas		
A.11.4.3	Identificación de equipos		
A.11.4.4	Puerto remoto de diagnóstico y configuración de protección		
A.11.4.6	Control para la conexión de redes		
A.11.6.2	Aislamiento del sistema sensible		
A.12.2.1	Validación de datos de entrada	Controles contra *malware*	A.10.4.1
A.12.2.2	Control de procesamiento interno		
A.12.2.3	Integridad de mensaje		
A.12.2.4	Validación de datos de salida		
A.12.5.4	Filtración de la información		
A.15.1.5	Prevención del uso indebido de las instalaciones para el procesamiento de información		
A.15.3.2	Protección de las herramientas de auditoría de sistemas de información		

Tabla 3. Controles eliminados en el Anexo A

Y por último, en la siguiente tabla se reflejan los nuevos controles incluidos en el Anexo A (García, 2013) (Trejo, ISO-27001:2013 ¿Qué hay de nuevo?, 2013):

Control	Descripción	Absorbe los controles de la ISO 27001:2005
A.6.1.4	Seguridad de la información en la gestión de proyectos	
A.12.6.2	Restricciones en la instalación de software	
A.14.2.1	Política de desarrollo de seguridad	
A.14.2.5	Desarrollo de procedimientos para el sistema	
A.14.2.6	Desarrollo de un entorno seguro	
A.14.2.8	Sistema de prueba de seguridad	
A.15.1.1	Información de seguridad para las relaciones de proveedores	A.6.2.3
A.15.1.3	Cadena de suministro ICT	
A.16.1.4	Evaluación y decisión de los eventos de seguridad de la información	

A.16.1.5	Respuesta a incidentes de seguridad de la información	
A.17.1.2	Implementación de la continuidad de la seguridad de la información	
A.17.2.1	Disponibilidad de las instalaciones para procesamiento de información.	

Tabla 4. Nuevos controles en el Anexo A

4.2 UNE-ISO/IEC 27002:2014

Es un código de buenas prácticas para la gestión de la seguridad de la información, donde se establece la metodología (requisitos para el inicio, implementación, mantenimiento y mejora) a seguir para implementar los controles de seguridad.

Está dividida en:

- **14 dominios.** Divisiones generales de ámbitos de la seguridad informática.

- **35 Objetivos de Control.** Subdivisiones de los dominios donde se establecerán apartados dedicados a varios aspectos concretos de cada uno de ellos. Únicamente informativos.

- **113 Controles.** Aspectos específicos a tratar directamente, que se encuentran englobados dentro de los objetivos de control, y que limitan las acciones a implementaciones concretas, y ayudan al consultor a realizar una interpretación específica y detallada de las necesidades.

El ANEXO A de la ISO 27001 contiene los mismos controles que los detallados en la ISO 27002, habiendo tan sólo dos diferencias:

1. La numeración de los controles de la ISO 27001 y 27002 son exactamente iguales, salvo que los reflejados en el ANEXO A, llevan una “A” precediéndoles.

2. El nivel de detalle, en la ISO 27001 solamente se hacen referencia a los mismos y en la ISO 27002 se detalla cómo implementar el control.

Estos controles se pueden dividir en varias tipologías:

- **Controles Técnicos.** Supervisan todos aquellos ámbitos relacionados con la seguridad física y lógica.

- **Controles de Gestión y organización.** Tienen como objetivo a los activos humanos, y se centran en los procedimientos, metodologías internas, responsabilidades etc…

- **Controles Legales.** Persiguen cubrir la obligación de cumplimiento de la normativa y legalidad específica para la organización en tema de seguridad de la información.

Según los análisis previos que se hayan realizado y la evaluación de riesgos, seleccionaremos los controles a implementar y, según la partida presupuestaria de la organización para el proyecto y las características de la misma, se realizarán con mayor detenimiento y dedicación o de una manera más superficial.

Toda exclusión de controles debe de ser justificada mediante evidencia de que los riesgos a los que atañe el control son asumidos por el responsable o no aplicables, esta exclusión debe quedar reflejada en el documento llamado Declaración de Aplicabilidad. La exclusión no justificada de un control u objetivo sería una “no conformidad” si se desea certificar el SGSI.

1. Proceso de adaptación a la norma ISO 27001

A partir de este punto, se ha desarrollado una guía en forma de documento para que pueda ser utilizada como punto de partida para que una consultora se certifique en la norma 27001:2013 y pueda cumplir todos los requisitos que la norma exige.

1.1 Objeto

El desarrollo e implantación de un Sistema de Seguridad de la Información (SGSI) ha sido una decisión estratégica tomada por Internel Group. Para ello, se han tenido en cuenta las diferentes necesidades, objetivos particulares, los servicios que ofrece, los procesos que para ello emplea, así como su estructura organizativa para poder:

- Demostrar su capacidad para proporcionar de forma segura unos servicios que satisfagan los requisitos del cliente y los requisitos legales.

- Aumentar la confianza de nuestros clientes a través de una aplicación eficaz de este sistema, incluyendo los procesos de mejora continua y la conformidad con los requisitos del cliente y los requisitos legales.

El SGSI basado en la norma ISO/IEC 27001 se documenta en el presente Manual de Seguridad, donde se hace referencia al resto de documentación que compone el Sistema y lo desarrolla.

1.2 Ámbito de aplicación

Internel Consulting, en adelante Internel, es una empresa del ámbito de las Tecnologías de la Información.

Los empleados de Internel se apoyan mutuamente para realizar Servicios de TI a clientes externos. Una parte importante de esta relación la constituye el proceso de Soporte Interno: los Sistemas de Información para el Acceso y Uso Seguro del Correo, de la Intranet Corporativa, de la Gestión de Incidencias, de la Monitorización y de los Equipos de los Técnicos dentro del alcance.

Toda esta documentación es de aplicación a todos los ámbitos de la organización bajo el alcance del SGSI o que tengan incidencia en el mismo. El Alcance del SGSI desarrollado e implantado en Internel contempla las siguientes actividades:

- LOS SISTEMAS DE INFORMACIÓN necesarios en la prestación de servicios cloud computing, consultoría, integración y explotación de sistemas e infraestructuras informáticos y outsourcing de sistemas de información a los clientes, DE ACUERDO A LA DECLARACIÓN DE APLICABILIDAD VIGENTE.

Debido a la naturaleza de los servicios que la organización suministra y/o gestiona, a las características de los requisitos de los clientes, a los requisitos legales aplicables, el SGSI de INTERNEL no considera la exclusión de ningún requisito de la norma de referencia, salvo aquellos puntos del Anexo A de la norma ISO/IEC 27001 que no sean de aplicación de manera justificada. La aplicabilidad de controles se establece de manera documentada en la Declaración de Aplicabilidad.

1.3 Objetivo

Internel ha implantado el Sistema de Gestión de la Seguridad de la Información con el objetivo de demostrar su capacidad para proporcionar de forma coherente servicios que satisfagan los requisitos del cliente y los reglamentarios aplicables. Así mismo, aspira a aumentar la satisfacción del cliente a través de la aplicación eficaz del sistema, incluidos los procesos para la mejora continua del sistema y el aseguramiento de la conformidad con los requisitos del cliente y los reglamentarios aplicables.

1.4 Definiciones

⇒ Acción Correctiva: Acción tomada para eliminar la causa de la no conformidad detectada u otra situación indeseable

⇒ Corrección: Acción tomada para eliminar una no conformidad detectada

⇒ No Conformidad: Incumplimiento de un requisito

⇒ Acción Preventiva: Acción tomada para eliminar las causas de una no conformidad potencial u otra situación potencialmente indeseable

⇒ Auditoría de Seguridad: Proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de auditoría

⇒ Aceptación del riesgo (ISO/IEC Guide 73: 2002): Decisión de aceptar un riesgo.

⇒ ACLs (Access Control List): Tabla que utilizan los sistemas para conocer los derechos de acceso que cada usuario posee para un objeto determinado, como directorios, ficheros, puertos, etc. Técnicas para limitar el acceso a los recursos según la información de autenticidad y las normas de acceso.

⇒ Activo (ISO/IEC 13335-1:2004): Cualquier cosa que tiene valor para la organización. [Magerit versión 3. 2012] Recursos de los sistemas de información o relacionados con éstos, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.

⇒ AGR: Análisis y gestión de riesgos.

⇒ Amenaza (ISO/IEC 13335-1: 2004): Una potencial causa de un incidente no deseado, el cual puede ocasionar un daño a un sistema o a la organización. [Magerit versión 3. 2012] Eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

⇒ Análisis de impacto [Magerit versión 3. 2012]: Estudio de las consecuencias que tendría una parada de X tiempo sobre la organización. [ISACA/CISM] Es un estudio para priorizar la criticidad de los recursos de información para una organización con base en los costos (o consecuencias) de eventos adversos. Se identifican amenazas a los activos y se determinan pérdidas de negocio potenciales para diferentes periodos.

⇒ Análisis de riesgos [Magerit versión 3. 2012]: Identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información (conocidos como 'activos'); para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.

⇒ Análisis del impacto de negocio (BS25999-1): Proceso de analizar las funciones de negocio y los efectos que una interrupción de negocio podría provocar sobre ellas. (ISACA/CISM). Evaluar la criticidad y la sensibilidad de los activos de información. Un ejercicio que determina el impacto de perder el soporte de cualquier recurso de una organización, establece el aumento de dicha perdida con el tiempo, identifica los recursos mínimos que es necesario recuperar y prioriza la recuperación de los procesos y sistemas de soporte.

⇒ Análisis del riesgo (ISO/IEC Guide 73: 2002): Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

⇒ Centro de respaldo ISACA/CISM: Es una instalación alterna para continuar con las operaciones de TI/SI cuando el centro principal no está disponible.

⇒ Confidencialidad (ISO/IEC 13335-1:2004): Propiedad de la información por la que ésta no se muestra disponible o revelada para individuos, entidades o procesos no autorizados. (ISACA/CISM). La protección de información privada o sensible contra divulgación no autorizada. [Magerit versión 3. 2012] Característica que previene contra la divulgación no autorizada de activos del dominio.

⇒ Continuidad de negocio (BS25999-1): Capacidad táctica y estratégica, Pre-aprobada por la gestión de una organización, para planear y responder a incidentes y a interrupciones de negocio para continuar con las operaciones de negocio en un aceptable nivel predefinido.

⇒ Control/es Medios de gestión del riesgo, que incluyen políticas, procedimientos, directrices, prácticas o estructuras de la organización, y que pueden ser de naturaleza administrativa, técnica, de gestión o legal. (ISACA/CISM) Las políticas, procedimientos, prácticas, dispositivos y estructuras organizacionales diseñadas para brindar una certeza razonable de que se alcanzarán los objetivos de negocio y que los eventos no deseados se prevendrán, o bien, se detectarán y corregirán. (COBIT) Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para proporcionar una garantía razonable de que los objetivos del negocio se alcanzarán y los eventos no deseados serán prevenidos o detectados.

⇒ Control de acceso (RLOPD): Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos. (ISACA/CISM) Las reglas, procedimientos, prácticas y dispositivos cuyo objetivo es prevenir la entrada o el derecho de uso no autorizado, ya sea físico o electrónico. (COBIT) El proceso que limita y controla el acceso a los recursos de un sistema computacional; un control lógico o físico diseñado para brindar protección contra la entrada o el uso no autorizados.

⇒ Copia de respaldo (RLOPD): Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

⇒ Datos de carácter personal (Reglamento de Desarrollo 1720/2007): Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

⇒ Declaración de la aplicabilidad: Declaración documentada que describe los objetivos del control y los controles que son relevantes y aplicables al SGSI de la organización.

⇒ Degradación: Pérdida de valor de un activo como consecuencia de la materialización de una amenaza.

⇒ Dimensión (de seguridad): Un aspecto, diferenciado de otros posibles aspectos, respecto del que se puede medir el valor de un activo en el sentido del perjuicio que causaría su pérdida de valor.

⇒ Disponibilidad (ISO/IEC 13335-1:2004): Propiedad de ser accesible y utilizable a demanda de una entidad autorizada. (ISACA/CISM) Garantizar que los sistemas de información y los datos estén listos para su uso cuando se les necesita; a menudo se expresa como el porcentaje de tiempo que se puede utilizar un sistema para trabajo productivo. [Magerit versión 3. 2012] Característica que previene contra la denegación no autorizada de acceso a activos del dominio.

⇒ DMZ (ISACA/CISM): La zona búfer entre la Internet y la red privada que tiene una ingeniería que utiliza en los firewalls y otros dispositivos para evitar el acceso de partes externas a los sistemas internos.

⇒ Encargado de tratamiento (LOPD): Persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

⇒ Evaluación del riesgo (ISACA/CISM): Un proceso que se utiliza para identificar y evaluar los riesgos y su posible impacto en la organización en términos cuantitativos o cualitativos. (ISO/IEC Guide 73: 2002). Procedimiento basado en el análisis del riesgo para determinar si se ha conseguido un riesgo tolerable.

⇒ Evento de seguridad de la información (ISO/IEC TR18044:2004). Una ocurrencia identificada de un sistema, servicio o red indicando una posible ruptura de la política de seguridad de la información o fallo de las salvaguardas, o una situación previamente conocida que pueda ser importante desde el punto de vista de la seguridad.

⇒ Fichero automatizado (LOPD): Todo conjunto organizado de datos de carácter personal que sean objeto de un tratamiento automatizado, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

⇒ Firewall (ISACA/CISM): Un sistema o una combinación de sistemas que impone una barrera entre dos o más redes que por lo regular forman una barrera entre un ambiente seguro y uno abierto, como la Internet.

⇒ Frecuencia: Tasa de ocurrencia de una amenaza.

⇒ Gestión de riesgos [Magerit versión 3. 2012]: Selección e implantación de las medidas o 'salvaguardas' de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. La gestión de riesgos se basa en los resultados obtenidos en el análisis de los riesgos.

⇒ Hot site (ISACA/CISM): Un sitio externo completamente operativo para el procesamiento de datos equipado con software de sistemas y hardware para su uso en caso de un desastre.

⇒ Hosting: Servicio de alojamiento de las páginas web que gestionan empresas especializadas. Las empresas que se dedican a este servicio son como los hoteleros de la red: ofrecen espacio para que otras compañías almacenen cualquier información que quieran que sea accesible por una red, desde sus páginas web hasta la información de su red interna o Intranet.

⇒ Housing: Alquiler de un espacio físico de un centro de datos para ubicar los equipos informáticos de la empresa

⇒ Identificación (RLOPD): Procedimiento de reconocimiento de la identidad de un usuario.

⇒ Impacto (BS25999-1): Consecuencia evaluada de un resultado particular. [Magerit versión 3. 2012]. Consecuencia que sobre un activo tiene la materialización de una amenaza.

⇒ Impacto residual. Impacto remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información.

⇒ Incidencia (RLOPD): Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

⇒ Incidente (BS25999-1): La situación que pudo ser, o podría conducir a, una interrupción del negocio, una interrupción, una pérdida, un incidente de emergencia o una crisis. Evento con consecuencias en detrimento de la seguridad del sistema de información.

⇒ Incidente de seguridad de la información (ISO/IEC TR 18044: 2004): Un único o una serie de eventos de seguridad no deseados ni esperados que tienen una significativa probabilidad de comprometer el funcionamiento del negocio y amenazar la seguridad de la información.

⇒ Información: Datos que poseen significado.

⇒ Integridad (ISO/IEC 13335-1:2004): Propiedad de salvaguardar la exactitud y la completitud de los activos. (ISACA/CISM) Cuan precisa, completa y valida es la información. [Magerit versión 3. 2012] Característica que previene contra la modificación o destrucción no autorizadas de activos de la organización.

⇒ ITIL (COBIT): Librería de infraestructura de TI de la oficina de gobierno gubernamental del reino unido (OGC).Un conjunto de lineamientos sobre la administración y procuración de servicios operativos de TI.

⇒ Madurez (COBIT): Indica el grado de confiabilidad o dependencia que el negocio puede tener en un proceso, al alcanzar las metas y objetivos deseados.

⇒ Malware: Cualquier programa cuyo objetivo sea causar daños a ordenadores, sistemas o redes y, por extensión, a sus usuarios

⇒ Mapa de riesgos: relación de las amenazas a que están expuestos los activos.

⇒ Métrica (COBIT): Un estándar para medir el desempeño contra la meta.

⇒ Métrica de seguridad (ISACA/CISM): Una forma de medición que se utiliza para determinar cualquier aspecto de la operación de cualquier actividad relacionada con la seguridad.

⇒ Modelo de valor: Caracterización del valor que representan los activos para la organización así como de las dependencias entre los diferentes activos.

⇒ Objetivo del Tiempo de Recuperación (RTO) (BS25999-1): Tiempo fijado para la reasunción de la entrega del producto, del servicio o de la actividad después de un incidente. (ISACA/CISM): Tiempo establecido para la recuperación de una función o recurso de negocio después de que ha ocurrido un desastre.

⇒ Plan de continuidad de negocio (PCB) (BS25999-1): Colección documentada de procedimientos y información que es desarrollada, compilada y mantenida para estar preparados ante la aparición de un incidente permitiendo que una organización continúe entregando sus productos críticos y servicios.

⇒ Plan de gestión de incidentes (BS25999-1): Plan de acción bien definido y documentado que se usa a la hora de un incidente, cubriendo típicamente las claves personales, los recursos, los servicios y las acciones que necesitan poner el proceso de gerencia en ejecución del incidente.

⇒ Política (ISACA/CISM): Declaraciones de alto nivel sobre el propósito y la dirección de la gerencia. (COBIT) Por lo general, un documento que ofrece un principio de alto nivel o una estrategia a seguir. El propósito de una política es influenciar y guiar la toma de decisiones presente y futura, haciendo que estén de acuerdo a la filosofía, objetivos y planes estratégicos establecidos por los equipos gerenciales de la empresa. Además del contenido de la política, esta debe describir las consecuencias de la falta de cumplimiento de la misma, el mecanismo para manejo de excepciones y la manera en que se verificará y medirá el cumplimiento de la política.

⇒ Privacidad (ISACA/CISM): Libertad contra intrusión o divulgación no autorizada de información sobre personas.

⇒ Procedimiento (ISACA/CISM): Una descripción detallada de los pasos necesarios para realizar operaciones especificas conforme a las normas aplicables. (COBIT) Una descripción de una manera particular de lograr algo; una forma establecida de hacer las cosas; una serie de pasos que se siguen en un orden regular definido, garantizando un enfoque consistente y repetitivo hacia las actividades.

⇒ Propietarios de datos (COBIT): Individuos, por lo general gerentes o directores, que tienen la responsabilidad de la integridad, el uso y el reporte preciso de los datos computarizados.

⇒ Propietario de riesgo: Persona(s) o entidad con responsabilidad y autoridad para gestionar un riesgo.

⇒ Responsable de seguridad (RLOPD): Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

⇒ Responsable del fichero (LOPD): Persona física o jurídica, de naturaleza pública o privada u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

⇒ Riesgo (ISO/IEC Guide 73: 2002): Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias. (COBIT) El potencial de que una amenaza específica explote las debilidades de un activo o grupo de activos para ocasionar pérdida y/o daño a los activos. Por lo general se mide por medio de una combinación del impacto y la probabilidad de ocurrencia. [Magerit versión 3. 2012] Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

⇒ Riesgo acumulado: Dícese del riesgo calculado resultado de tomar en consideración el valor propio de un activo y el valor de los activos que depende de él. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma.

⇒ Riesgo residual (ISO/IEC Guide 73: 2002): Riesgo remanente que existe después de que se han tomado las medidas de seguridad. [Magerit versión 3. 2012] Riesgo que se da tras la aplicación de salvaguardas dispuestas en un escenario de simulación o en el mundo real.

⇒ Risk Assessment (BS25999-1): Proceso total de la identificación, del análisis y de la evaluación del riesgo.

⇒ RLOPD (RLOPD): Real Decreto 1720/2007 de 21 de Diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal.

⇒ Single Sign On (SSO): Concepto que consiste en la autenticación única por parte del usuario para acceder a sus recursos. La idea es introducir una única vez el nombre de usuario y contraseña, sin necesidad de volver a facilitarlo a la hora de acceder a nuevos recursos en los que aún no se había autenticado.

⇒ Software antivirus (ISACA/CISM): Un software de aplicación utilizado en múltiples puntos en una arquitectura de TI diseñado para detectar y posiblemente eliminar códigos de virus antes de que ocasionen algún daño, así como reparar o poner en cuarentena los archivos que ya han sido infectados.

⇒ Salvaguarda: Procedimiento o mecanismo tecnológico que reduce el riesgo.

⇒ Seguridad: La capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos así como de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

⇒ Seguridad de la información (ISO/IEC 27002: 2005): La preservación de la confidencialidad, integridad y disponibilidad de la información. Pueden estar involucradas, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y fiabilidad.

⇒ Servicio de la sociedad de la información (LSSICE): Todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.

⇒ Sistemas de detección de intrusos (IDS) (ISACA/CISM): Un IDS inspecciona la actividad en la seguridad del host y la red para identificar patrones sospechosos que pudieran ser indicadores de un ataque al sistema o la red.

⇒ Sistema de Gestión de Seguridad de la Información (SGSI): Aquella parte del sistema global de gestión, basada en una aproximación del riesgo de negocio, para establecer, implantar, poner en marcha, controlar, revisar, mantener y mejorar la seguridad de la información.

⇒ Sistemas de información [Magerit versión 3. 2012]: Conjunto de elementos físicos, lógicos, elementos de comunicación, datos y personal que permiten el almacenamiento, transmisión y proceso de la información. (RLOPD) Conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

⇒ SLA (COBIT): Acuerdo de nivel de servicio. Acuerdo por escrito entre un proveedor de servicios y los usuarios del cliente, el cual documenta los niveles de servicio acordados para un servicio prestado.

⇒ Soporte (RLOPD): Objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

⇒ Spam: Mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas que perjudican de una u otra manera al receptor. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.

⇒ Spyware: Software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

⇒ SSL (Secure Sockets Layer): Protocolo criptográfico que proporciona comunicaciones seguras en Internet. Proporciona autenticación y privacidad de la información entre extremos de comunicación sobre Internet mediante el uso de criptografía.

⇒ Tratamiento De Datos (LOPD): Operaciones y procedimiento técnicos, de carácter automatizado que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

⇒ Tratamiento del riesgo: Proceso de selección y de implantación de medidas para modificar el riesgo.

⇒ Trazabilidad: Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.

⇒ Troyano: Programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema en el que se introduce de manera subrepticia (de ahí su nombre).

⇒ Valor de un activo. Es una estimación del coste inducido por la materialización de una amenaza.

⇒ Valor acumulado: Considera tanto el valor propio de un activo como el valor de los activos que dependen de él.

⇒ Valoración del riesgo (ISO/IEC Guide 73: 2002): Proceso global de análisis y evaluación del riesgo.

⇒ Virus informático: Es un programa o software que se auto ejecuta y se propaga insertando copias de sí mismo en otro programa o documento.

⇒ VLAN (Virtual LAN): Es una red de computadoras lógicamente independiente. Varias VLANs pueden coexistir en un único switch físico. Se comportan como si estuviesen conectados al mismo cable, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local.

⇒ VPN (Red privada virtual) (ISACA/CISM): Una red privada segura que utiliza la infraestructura de las telecomunicaciones públicas para transmitir datos. En comparación con un sistema mucho más costoso de líneas propias o rentadas que solo pueden ser utilizadas por una compañía, las VPN son utilizadas por empresas tanto para extranets como para áreas amplias de Intranets. Mediante el uso de cifrado y autenticación, una VPN cifra todos los datos que pasan entre dos puntos de Internet, manteniendo la privacidad y la seguridad.

⇒ Vulnerabilidad (ISO/IEC 13335-1: 2004): Una debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas. [Magerit versión 3. 2012] Vulnerabilidad de un activo es la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.

⇒ Warm site (ISACA/CISM): Es similar a un hot site; sin embargo, no está completamente equipado con todo el hardware necesario para la recuperación.

1.5 Documentación del SGSI

A continuación se lista toda la información documentada que una empresa debe generar dentro del ámbito del SGSI:

⇒ MANUALES Y PROCEDIMIENTOS GENERALES

- ⇒ Manual de Gestión de Seguridad
- ⇒ Revisión por la Dirección
- ⇒ Control de documentación y registros
- ⇒ Manual General de Recursos Humanos y Materiales
- ⇒ Revisión del Equipo Humano
- ⇒ Gestión de Compras
- ⇒ Medición Análisis y Mejora
- ⇒ Gestión de No Conformidad, Reclamaciones de Clientes, Acciones Preventivas y Correctivas
- ⇒ Auditorías del Sistema de Gestión Integrado
- ⇒ Manual de Políticas de Seguridad
- ⇒ Manual de Políticas para usuarios
- ⇒ Declaración de Aplicabilidad
- ⇒ Procedimiento Análisis y Gestión de Riesgos
- ⇒ Procedimiento de Comunicación

⇒ PROCEDIMIENTOS ESPECÍFICOS

- ⇒ Clasificación y Tratamiento de Activos
- ⇒ Seguridad Física y del Entorno
- ⇒ Gestión de Comunicaciones y Operaciones
- ⇒ Control de Accesos
- ⇒ Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
- ⇒ Gestión de Incidentes de Seguridad
- ⇒ Plan de Continuidad de Negocio y Planes de Contingencia
- ⇒ Conformidad Legal y Reglamentaria
- ⇒ Gestión de Dispositivos móviles
- ⇒ Criptografía
- ⇒ Seguridad en Gestión de Proyectos

1.6 Presentación de la empresa

Internel tiene como misión ofrecer servicios de consultoría e integración especializados en Tecnología y Sistemas de Información, principalmente orientados a aportar las soluciones necesarias en las áreas de Informática, Telecomunicaciones y Telemática, con la vocación de conseguir la excelencia y satisfacción en las necesidades de productividad y competitividad de nuestros clientes.

Nace en 2015, de la asociación de cualificados profesionales de la consultoría técnica, con un dilatado bagaje profesional en diversas compañías nacionales y multinacionales, líderes en sus respectivos sectores.

Actualmente dispone de una plantilla eminentemente técnica compuesta por en torno a una decena de profesionales que desempeñan cometidos de Jefes de Proyecto, Consultores y Técnicos, cubriendo el ámbito de la geografía nacional.

1.7 Contexto de la organización

1.7.1.- Comprensión de la Organización y su contexto

INTERNEL determinará las cuestiones externas e internas relevantes para sus propósitos y actividades que afecten a su capacidad para conseguir el resultado esperado de su SGSI.

Toda esta información se tendrá presente siempre que se establezca, implemente, y mantenga el SGSI de la organización.

INTERNEL ha identificado y documentado lo siguiente:

a) Las actividades de la organización, funciones, servicios, productos, asociaciones, cadenas de suministro, las relaciones con las partes interesadas. Las relaciones con partes interesadas pueden consultarse en el registro: *Partes interesadas y riesgos asociados*.
   Los servicios y productos realizados por INTERNEL se encuentran detallados en el punto de *Alcance-SGSI*.
   Con respecto a suministros, se dispone de un registro actualizado de proveedores: *Evaluación proveedores*.

b) Las relaciones entre la política de seguridad, los objetivos de la organización y otras políticas, incluyendo su estrategia global de gestión de riesgos.

c) El nivel de riesgo aceptable de la organización.

Para establecer su contexto, la organización:

- Articulará sus objetivos relativos a la Seguridad de la Información.
- Definirá los factores externos e internos que crean la incertidumbre que da lugar a riesgo.
- Establecerá criterios de riesgo, teniendo en cuenta el apetito del riesgo, y definirá el propósito del SGSI.

Asimismo, en las revisiones por la Dirección se establecen objetivos al menos con una periodicidad anual.

1.7.2.- Comprensión de las necesidades y expectativas de las partes interesadas

Al establecer el SGSI, INTERNEL ha establecido y delimitado:

a) Las partes interesadas que son relevantes para el SGSI.
b) Los requisitos de estas partes interesadas (es decir, sus necesidades y expectativas establecidas, generalmente implícitas u obligatorias).

Toda esta información queda recogida en el registro *Partes interesadas y riesgos asociados*, en la que se utiliza el documento *Metodología del Análisis y Gestión de Riesgos* para el cálculo del riesgo sobre las partes interesadas, en función de las diversas amenazas que pudieran afectar a las mismas.

1.7.2.1.- Cumplimiento de Requisitos Legales

INTERNEL tiene como objetivo en el marco de su SGSI el cumplimiento de toda legislación que le aplique, especialmente las normativas sobre Protección de Datos de Carácter Personal y sobre Propiedad Intelectual. Igualmente, INTERNEL quiere asegurarse el cumplimiento de cualquier otra legislación sectorial que le pudiera ser de aplicación.

De conformidad con lo indicado en la Ley Orgánica de Protección de Datos (LOPD), INTERNEL mantiene un *Documento de Seguridad* bajo la custodia y responsabilidad del Responsable de Seguridad.

Asimismo, en el procedimiento *Conformidad legal y reglamentaria*, establece el marco normativo al que INTERNEL se encuentra sujeta, de manera que se pueda llevar a cabo un control y un seguimiento constante de la legislación que se debe observar.

Toda esta información queda recogida en el registro *Partes interesadas y riesgos asociados.*

1.8 Alcance – SGSI

1.8.1.- Requisitos Generales

INTERNEL ha establecido, documentado e implantado, su SGSI, que está constituido por un conjunto de procesos, responsabilidades, actividades, recursos y procedimientos que permiten garantizar la confidencialidad, integridad y disponibilidad de la información que gestiona.

1.8.2.- Procesos

A continuación se muestra el Mapa de Procesos de Internel, donde se reflejan la interacción de los procesos estratégicos, operativos y de soporte a través de los cuales se satisfacen las necesidades de los clientes.

El alcance del SGSI queda definido como:

- LOS SISTEMAS DE INFORMACIÓN necesarios en la prestación de servicios cloud computing, consultoría, integración y explotación de sistemas e infraestructuras informáticos y outsourcing de sistemas de información, DE ACUERDO A LA DECLARACIÓN DE APLICABILIDAD VIGENTE.

1.8.3.- Ubicaciones

Los servicios de TI prestados desde las oficinas de la zona centro (Sede en Leganés), sitas en Av. de la Universidad, 30, 28911 Leganés, Madrid.

1.8.4.- Tecnologías

Se incluyen en el alcance las siguientes tecnologías, que soportan los procesos de negocio de Internel:

- Entorno virtual HYPER-V que soporta los siguientes sistemas:
  - Controlador Dominio primario y copia.
  - Gestor documental frontal y base de datos.
  - Citrix.
  - Servidor de Archivos.
  - Servidor de Backup.
  - Servidor Correo.
  - Servidor Monitorización.
- Comunicaciones
  - Conexión internet.
  - Conexión VPN con Datacenter.
  - Arquitectura de firewalls.
  - Red Local.
- Almacenamiento
  - Almacenamiento EMC2.
  - Red de fibra.
- Entorno Cloud.
  - Skype for bussines.
  - Yammer.

1.8.5.- Requisitos legales

El listado de requisitos legales se encuentra de manera detallada en el registro *Partes interesadas y riesgos asociados*.

1.8.6.- Partes interesadas

- Proveedor CPD Principal: GLOABL SWITCH.
- Fabricantes y distribuidores hardware: DELL, SONICWALL, EMC, FUJITSU.
- Fabricantes y distribuidores software: MICROSOFT, CITRIX, VMWARE, SYMANTEC.
- Proveedor comunicaciones: TELEFONICA.

El listado completo de partes interesadas se encuentra en el registro *Partes interesadas y riesgos asociados*.

1.8.7.- Exclusiones

Quedan excluidos del alcance los siguientes elementos:

- Toda infraestructura (servidores y comunicaciones) de Internel o ajena que soporta los sistemas de información de negocio de clientes.
- Equipos de los usuarios que realizan exclusivamente las actividades de negocio de Internel en el cliente y se adaptan a las normas de seguridad del mismo (Consultoría, Integración, Cloud, Outsourcing).

1.9 Sistema de Gestión de Seguridad de la Información

La organización establece, implementa, mantiene y mejora continuamente el SGSI, de acuerdo con los requisitos fijados por la norma ISO 27001:2013.

Para ello, cuenta con los siguientes elementos:

- Métricas y mediciones (Seguimiento de Métricas del SGSI)
- Entradas/Salidas de las Revisiones por la Dirección
- Acciones correctivas/de mejora
- Fijación, Planificación y seguimiento de objetivos de Seguridad (registro *Planificación y Seguimiento de Objetivos*).
- Fijación, Planificación y Seguimiento de tareas del SGSI (registro *Planificación y seguimiento de tareas del SGSI*).
- Seguimiento de tareas del SGSI: *Responsables y Tareas en aplicación*

1.10 Liderazgo

1.10.1.- Liderazgo y compromiso

La Dirección demuestra su liderazgo asignando las funciones, y estableciendo obligaciones, contribuyendo siempre a mejorar la eficacia del SGSI.

Por ello, ha fijado una Política de Seguridad de la información, con intenciones y compromisos claros. Esta política se encuentra definida en el punto *Política de Seguridad de la Información*.

Conforme al SGSI, las funciones y obligaciones asignadas se han dado al conocer a todo el personal a través del documento *Manual de Políticas de Seguridad de la Información para Usuarios*.

1.11 Responsabilidad de la Dirección

1.11.1.- Compromiso de la Dirección

La Dirección de Internel proporciona evidencia de su compromiso con el desarrollo e implementación del Sistema de Gestión de Seguridad de la Información, así como con la mejora continua de su eficacia mediante las siguientes actividades:

- Comunicando a la organización la importancia de satisfacer tanto los requisitos del cliente, como los legales y reglamentarios.
- Estableciendo la política del SGSI, que se detalla en este Manual.
- Asegurando que se establecen los objetivos de seguridad.
- Llevando a cabo las revisiones por la Dirección.
- Asegurando la disponibilidad de recursos. La Dirección se compromete a proporcionar los recursos necesarios para el correcto desarrollo de las actividades desarrolladas por la Organización.

El Responsable del SGSI:

- Supervisa el cumplimiento de la Política de Seguridad de la Información de Internel para procesos identificados en el Alcance del SGSI, a todos los empleados y terceras partes relacionadas del SGSI.
- Trabaja de forma continuada en implementar modificaciones y/o mejoras al SGSI de Internel para acercar los resultados conseguidos a los planificados.
- Realiza las actualizaciones del análisis de riesgos del SGSI.
- Mide la satisfacción de los clientes del SGSI.

El Responsable del centro de servicios:

- Organiza y controla al personal y el hardware dentro del alcance del SGSI de forma que se cumplan los requisitos establecidos en la *Política de Seguridad de la Información*.

- Controla la generación y uso de procedimientos y registros de actividad.
- Coordina el Equipo de Recuperación de Desastres.

1.12 Política de Seguridad de la Información

La Dirección de Internel establece la Política de Seguridad de la Información siendo de aplicación para los procesos identificados en el Alcance del SGSI, a todos los empleados y terceras partes relacionadas.

La Dirección concretará los objetivos de seguridad de Internel anualmente en la Revisión del Sistema. Al fijar dichos objetivos, se establecerán los responsables, los medios y acciones necesarias a realizar para poder alcanzar los mismos.

Es responsabilidad de todos, la implantación y el seguimiento de la política de seguridad, comenzando por la Dirección, que marcará los criterios estratégicos a seguir.

El SGSI establece como objetivos generales los siguientes:

- Gestionar las principales dimensiones de seguridad de la información: confidencialidad, integridad y disponibilidad
- Cumplir con las necesidades y expectativas de las partes interesadas involucradas dentro del alcance del SGSI, preservando la Disponibilidad, Integridad y Confidencialidad de la información.
- Demostrar liderazgo por parte de la dirección asegurando que la política de Seguridad de la Información, y los objetivos de seguridad se establecen y son compatibles con la dirección estratégica de la organización.
- Servicios con un nivel de seguridad de la información que satisfagan y superen las necesidades de nuestros clientes.
- Prevención de posibles defectos y posibles incidentes de seguridad de la información antes de que ocurran, trabajando orientados hacia la “mejora continua” y la comunicación.
- Asegurar el cumplimiento de la legislación, reglamentación y normativas aplicables, así como todos aquellos requisitos que la organización considere oportunos.
- Asignación eficaz de funciones y responsabilidades en el ámbito de la seguridad.

- Servicios con un nivel de seguridad de la información que satisfagan y superen las necesidades de nuestros clientes.
- Prevención de posibles defectos y posibles incidentes de seguridad de la información antes de que ocurran, trabajando orientados hacia la "mejora continua" y la comunicación.
- Revisiones continuas del Sistema de Gestión de Seguridad de la Información.
- Establecimiento de indicadores de seguridad que nos permitan conocer el grado de seguridad de nuestros procesos productivos.
- Fomento de la formación del personal de la organización en los aspectos débiles que se detecten a lo largo del ejercicio.
- Realización de auditorías de seguridad periódicas para conocer el grado de cumplimiento de la política de seguridad.
- Establecer el nivel de seguridad basándose en análisis de riesgos y en los objetivos.
- Concienciación y motivación del personal sobre la importancia de una correcta gestión de la seguridad de la información.
- Analizar los riesgos a los que está expuesta la Organización, y gestionarlos de la mejor forma posible para alcanzar el nivel de riesgo aceptado por la Dirección. El SGSI proporciona los mecanismos para, basándose en la metodología MAGERIT, analizar y gestionar el riesgo, y determinar aquellos riesgos que la Organización considera aceptables.

Fecha: Septiembre de 2015

Javier Donoso. Director General

1.13 Funciones, Responsabilidades y Autoridades

1.13.1.- Responsabilidad y Autoridad

La Dirección de Internel se asegura de que las responsabilidades y autoridades de todo el personal que conforma la organización, estén definidas y sean comunicadas.

La organización de Internel, así como las responsabilidades concretas de su personal respecto del SGSI, quedan reflejadas en:

- El *Organigrama general*.
- La *Descripción del puesto de trabajo*.

1.13.2.- Representante de la Dirección

La responsabilidad del SGSI está asignada al Responsable de Seguridad.

El Responsable de Seguridad es responsable de verificar el cumplimiento de lo especificado en este Manual, recomendar soluciones y comprobar la puesta en práctica de las mismas cuando se produzcan desviaciones respecto a lo establecido en el SGSI. Para ello posee la autoridad y libertad necesarias, concedidas por la Dirección General de la Empresa.

Por otro lado, el Responsable de Seguridad también es el representante de la Dirección, que con independencia de otras competencias tiene responsabilidad y autoridad para:

- Asegurar que se establecen implantan y mantienen los procesos necesarios para el SGSI.
- Colaborar en la definición de la política de gestión, objetivos y planificación.
- Convocar al Comité de Dirección.
- Informar a Dirección sobre el desempeño del sistema y de cualquier necesidad de mejora que pueda surgir, a través del Comité o la Revisión del Sistema.
- Asegurar que se promueve la toma de conciencia de la importancia de cumplir con los requisitos del SGSI en las áreas de la empresa que quedan bajo el Alcance del SGSI, a través de las actividades de comunicación descritas
- Asegurar el cumplimiento técnico, legal y organizativo en materia de seguridad de la información en toda la organización.
- Actuar como enlace con terceras partes, como el organismo certificador, etc.

Para el desarrollo de sus funciones, tiene relación directa con los diversos responsables de Áreas o Departamentos y con cualquier persona que pueda incidir en la Seguridad de la Información del servicio prestado.

Los roles y responsabilidades se encuentran definidos en el registro *Estructura organizativa y perfiles profesionales*.

1.14 Planificación

1.14.1.- Acciones para abordar los riesgos y oportunidades

Al planificar el SGSI, la organización considera las cuestiones mencionadas en el punto *Contexto de la Organización*:

- Garantizar que el sistema de gestión puede alcanzar su resultado previsto,
- Evitar o reducir los efectos no deseados,
- Lograr la mejora continua.

La organización ha planificado acciones para hacer frente a estos riesgos y oportunidades:

- la forma de integrar e implementar las acciones en sus procesos dentro del alcance del SGSI,
- la forma de evaluar la eficacia de estas acciones (relacionado con seguimiento, medición, análisis y evaluación).

Toda esta información se encuentra relacionada de forma directa con el punto *Contexto de la Organización* del presente documento. Por ello se dispone del registro *Partes interesadas y riesgos asociados* en el que también se identifican riesgos y oportunidades, de cara a las partes interesadas.

1.14.2.- Gestión del Riesgo de la Seguridad de la Información

De forma adicional al proceso de identificación de riesgos de *Partes Interesadas* ya mencionado, la organización ha definido y aplicado un proceso de Gestión del Riesgo en el ámbito específico de Seguridad de la Información. Este proceso se rige por una metodología definida por INTERNEL, y presente en el documento: *Metodología de Análisis y Gestión de Riesgos*.

Dicha metodología:

- Consta de un criterio de aceptación del riesgo;
- Define los criterios de valoración del riesgo;

- Permite utilizar la herramienta PILAR, basada en MAGERITv3 para activos y una metodología basada en ISO 31000 para el análisis de contextos y partes interesadas, lo que asegura que la repetición de valoraciones del riesgo produzca resultados consistentes, válidos y comparables;
- Identifica los riesgos de Seguridad de la Información:
    - Aplicando un proceso de valoración del riesgo para identificar los riesgos asociados a la pérdida de confidencialidad, integridad o disponibilidad, dentro del alcance del SGSI;
    - Identifica los propietarios /responsables del riesgo (será el propietario/responsable del activo afectado por el riesgo);
- Analiza los riesgos de Seguridad de la Información:
    - Valorando las consecuencias potenciales que podrían ocurrir si un riesgo identificado se materializa;
    - Valora una probabilidad de ocurrencia de los riesgos identificados y determina el nivel de riesgo;
- Evalúa los riesgos de Seguridad de la Información:
    - Compara los resultados del análisis de riesgos con el criterio de riesgos establecido.
    - Prioriza el tratamiento del riesgo obtenido en *Análisis de Riesgos*.

1.14.3.- Tratamiento de los Riesgos de Seguridad de la Información

Se ha definido un proceso de tratamiento de los Riesgos de Seguridad de la Información identificados, el cual se define en el documento: *Metodología de Análisis y Gestión de Riesgos*.

Dicho proceso permite establecer acciones para tratar los riesgos identificados, en función de los controles que se consideren necesarios para mitigar el riesgo.

Los controles a implementar podrán pertenecer al Anexo A (ISO 27002), pero también podrán existir controles adicionales.

El nivel de riesgo aceptable se fijará en las reuniones de Revisión por la Dirección, delimitándose entonces los riesgos que deberán mitigarse.

1.14.4.- Objetivos de Seguridad y planes para alcanzarlos

Los objetivos de seguridad son responsabilidad de la Dirección de Internel, quien los define anualmente en las reuniones de Revisión por la Dirección, de acuerdo con la Política de Seguridad. Estos objetivos se registran en la revisión del SGSI por la dirección y son gestionados dentro de la organización, utilizando para ello la aplicación de gestión de incidencias corporativo.

Para facilitar la operativa con dichos objetivos, se elabora un documento de objetivos que se utiliza para planificarlos, describirlos con mayor detalle y facilitar su revisión, en el que se especifican los siguientes aspectos:

- Descripción general del objetivo.
- Metas para conseguir el objetivo
- Hitos
- Planificación.
- Forma de cálculo.
- Seguimiento.
- Responsables.
- Recursos

Las acciones correctivas que puedan desprenderse del seguimiento de objetivos, se tratan según lo dispuesto en el procedimiento de *No Conformidades, Reclamaciones de Clientes, Acciones Correctivas y Preventivas.*

La alta dirección se asegura que:

- La planificación del sistema de gestión de seguridad se realiza con el fin de cumplir con los requisitos citados en el apartado *Contexto de la Organización* de este documento, así como los objetivos de seguridad y se mantiene la integridad del sistema de gestión de seguridad cuando se planifican e implementan cambios en éste.
- El Responsable del SGSI realiza la planificación del sistema de gestión, especificando las acciones a realizar, la fecha de implantación, un responsable y un seguimiento.

El seguimiento de la planificación se lleva a cabo en la revisión por la dirección, en la cual se identifican las posibles alteraciones en el sistema así como el modo en que se ve afectado éste por la aparición de nuevas situaciones o cambios en las condiciones iniciales de la organización.

1.15 Gestión de los Recursos

1.15.1.- Provisión de Recursos

Internel determina los recursos necesarios para implementar y mantener al día el SGSI y mejorar continuamente su eficacia y aumentar la satisfacción del cliente mediante el cumplimiento de sus requisitos.

La Dirección de INTERNEL adquiere el compromiso de identificar y proporcionar los recursos necesarios para:

- Establecer, implementar, operar, supervisar, revisar, mantener y mejorar el sistema de gestión SGSI.
- Asegurar que los procedimientos de Seguridad de la Información respondan a los requisitos empresariales.
- Identificar y cumplir los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales.
- Mantener la seguridad adecuada mediante la aplicación correcta de todos los controles implantadas.
- Llevar a cabo revisiones, cuando sea necesarias, y reaccionar en base a los resultados de las mismas.
- Mejorar la eficacia del SGSI.

La identificación de los recursos necesarios podrá venir por distintas vías entre las que destacamos:

- A través de cualquiera de los responsables de las distintas áreas y unidades de INTERNEL.
- A propuesta del Comité de Dirección de Seguridad.
- Como consecuencia de sugerencias o no conformidades.
- Como consecuencia de las actividades de planificación de acciones de seguridad que se definan, en especial en la definición de los objetivos de Seguridad de cada año.

En el SGSI se han identificado en cada apartado que lo precisa, los recursos necesarios, que pueden ser:

- Recursos materiales: medios informáticos, instalaciones, etc.
- Recursos documentales: documentación del sistema (procedimientos, instrucciones o especificaciones técnicas), normas de referencia.
- Recursos humanos: personal con la competencia adecuada a las tareas a realizar.

1.15.2.- Recursos Humanos

1.15.2.1.- Generalidades

INTERNEL determina los medios necesarios para que el personal que realiza trabajos que afectan a la seguridad del servicio, sean competentes con base a la educación, formación, habilidades y experiencia apropiadas.

1.15.2.2.- Competencia

En relación a su personal, Internel realiza las siguientes actividades clave:

1. Determina la competencia necesaria para el personal que realiza trabajos que afectan a la seguridad del servicio. En este sentido, la organización de Internel deja reflejadas dichas necesidades en los perfiles de puesto, tal como se define en el documento: *Estructura Organizativa y Perfiles Profesionales*.

2. Internel proporciona una formación continua en el mismo puesto de trabajo, de modo que los empleados acceden a puestos superiores tras los periodos de aprendizaje necesarios y del éxito determinado en cada caso. Este proceso se define en el documento *Revisión del Equipo Humano* y se registra en las revisiones a los empleados que se realizan, las cuales constan de revisiones funcionales y salariales, si procede.

   Las necesidades de formación se detectan a través de diferentes fuentes:

- Determinada y detectada por sus superiores dependiendo de las características del puesto que ocupa, según la definición de perfiles descrita en el documento: Estructura organizativa y perfiles profesionales.
- Determinando las necesidades del mercado: nuevas tecnologías, exigencias de clientes y proyectos, etc.
- A demanda del propio empleado, que es evaluada convenientemente por el responsable de dicho empleado.

3. Una vez detectadas las necesidades de formación de cada departamento, el Responsable de Seguridad añade las acciones formativas en el Registro de Actividades de Formación, que incluye todas las actividades previstas y realizadas en cuestiones de formación y evalúa la eficacia de las acciones formativas.

   Para evaluar el grado de eficacia de las acciones formativas emprendidas por Internel, el Responsable de Seguridad realiza las siguientes actividades:

   - Revisa el Seguimiento de la Formación: Durante la reunión de revisión del Sistema de Gestión por la Dirección, el Responsable de Seguridad, junto con el resto de los integrantes del comité, determina el grado de cumplimiento de las acciones formativas planificadas.
   - Se asegura de que el personal es consciente de la pertenencia e importancia de sus actividades y de cómo contribuyen al logro de los objetivos de seguridad.
   - Mantiene registros apropiados de la educación, formación, habilidades y experiencia.

1.15.3.- Concienciación

Las personas que realizan trabajos bajo el control de la organización tendrán en cuenta en todo momento:

- La política de Seguridad de la Información,
- Su contribución a la eficacia del SGSI, incluyendo los beneficios de la gestión de la mejora continua,

- Las consecuencias de que no cumplan con los requisitos del SGSI

Mediante la intranet local, el grupo de seguridad publica noticias relevantes respecto a la seguridad de la información. Adicionalmente se definen acciones ad-hoc para concienciar al personal sobre alguna cuestión o temática específica.

1.15.4.- Comunicación

La organización determina la necesidad de comunicaciones internas y externas relacionadas con el SGSI, incluyendo:

- Sobre qué comunicar
- Cuando comunicar
- Con quien comunicarse
- Qué comunicar, y
- Los procesos mediante los que las comunicaciones son efectuadas.

Las comunicaciones del sistema de gestión de Seguridad de la Información enviadas y recibidas de/a partes interesadas que se consideren relevantes se documentarán a modo de registro del SGSI.

Se facilita en todo momento la comunicación con las autoridades pertinentes, garantizando la interoperabilidad y respuesta de la organización y del personal.

Se incluyen dentro de las pruebas periódicas, los elementos que se utilizan para establecer las comunicaciones en caso de interrupción de las comunicaciones normales, garantizando así su capacidad y disponibilidad.

Para cumplir con todo lo estipulado, se han documentado procedimientos de comunicación, que pueden consultarse en el documento *Procedimiento de Comunicación*.

1.16 Requisitos de la Documentación

1.16.1.- Generalidades

La documentación del sistema de gestión de seguridad de la información de Internel está compuesto por:

- Declaración documentada de la Política del SGSI y de los Objetivos de Seguridad.
- El *Manual de Seguridad*, que constituye el documento básico del Sistema de Gestión de la Seguridad de la organización y donde se describe de manera general cómo se asegura por parte de Internel el cumplimiento de los requisitos de la norma de referencia.
- Los procedimientos documentados requeridos expresamente por esta norma. En ellos se desarrolla con mayor detalle (cuando sea procedente) los aspectos integrados en el manual.
- Los documentos necesitados por la organización para asegurarse de que sus procesos cuentan con una planificación, operación y control eficaz.
- Los registros de esta norma.

1.16.2.- Manual de Seguridad

El Manual de Seguridad es un documento dinámico que describe el Sistema de Gestión de Seguridad de la Información de Internel de forma global y para cada apartado de la norma ISO 27001.

El Manual de Seguridad es realizado por el Responsable del SGSI y aprobado por la Dirección de la Organización.

El Manual de Seguridad, junto con los procedimientos, constituye la base para asegurar que la organización es capaz de cumplir efectivamente con los requisitos pactados con las terceras partes (clientes, empleados, accionistas, proveedores, administración, el Estado a través de la legislación y reglamentos, etc.)

El Manual de Seguridad hace referencia a los procedimientos generales y específicos y a cómo se relacionan con cada uno de los apartados de la norma.

1.16.3.- Control de documentación y registros

Internel tiene establecido un procedimiento general para describir los controles necesarios para los diferentes tipos de documentos utilizados en el sistema de gestión de la calidad. (Control de la Documentación y de los Registros).

La actuación de Internel respecto al control de la documentación se concreta en los siguientes aspectos:

- Considerar que los documentos de seguridad son esenciales para la correcta gestión y la realización de las diferentes actividades del sistema de seguridad.
- Asegurar que cada uno de los documentos está en su versión vigente, disponible donde se necesita y a la disposición de aquellos que los deban utilizar o consultar.

Para asegurar el control de los documentos relacionados con la Seguridad, la Organización realiza las siguientes actividades:

- Mantiene al día el registro *Estructura Documental*, en el que se registran todos los documentos de la organización, incluidos los relativos al Sistema de Gestión de Seguridad de la Información.
- Identifica los Procedimientos Generales, el Manual de Seguridad y resto de documentos mediante el nombre, la fecha y su versión.
- Se asegura que las versiones vigentes están disponibles para quien las necesita.
- Controla la distribución y retirada de documentación obsoleta. La documentación del sistema de seguridad se encuentra disponible en carpetas y se distribuye por medio del Responsable del SGSI, quién se encarga de retirar la documentación obsoleta.

Se asegura que los documentos externos se identifican y distribuyen a aquellos que los necesitan.

1.17 Operación

1.17.1.- Planificación, Operativa y Control

La organización planifica, ejecuta y controla los procesos necesarios para cumplir los requisitos, e implementa las acciones determinadas en el punto

Acciones para abordar riesgos y oportunidades del punto de *Planificación*. Para ello se utiliza el documento Excel *Planificación Centro de Servicios*.

Por otro lado, también se han implementado unos planes para lograr los objetivos de seguridad determinados en el punto *Objetivos de Seguridad de la Información*.

La organización controla y planifica, a través de la gestión de cambios, los cambios realizados y revisa las consecuencias de los mismos y la adopción de medidas para mitigar los efectos adversos, en el caso de que fuera necesario.

La organización debe asegurarse de que los procesos externalizados están controlados.

El siguiente esquema representa de forma detallada las acciones que se llevan a cabo dentro de los procesos necesarios para cumplir con los requisitos del SGSI:

1.17.2.- Operación: Análisis del Riesgo de la Seguridad de la Información

La organización establece, implementa y mantiene un proceso formal y documentado para el análisis de riesgos, establecido en el punto de *Planificación* del presente documento.

La metodología utilizada contempla la operación del Análisis del Riesgo, y se encuentra descrita en el procedimiento *Metodología de Análisis y Gestión de Riesgos*.

1.17.3.- Operación: Tratamiento del Riesgo de la Seguridad de la Información

La organización ha implementado un plan de tratamiento de Riesgos que asegura la efectividad del SGSI.

En el documento *Metodología de Análisis y Gestión de Riesgos* también se especifica el proceso de tratamiento del riesgo.

Se guarda como el registro *Plan de Tratamiento de Riesgos_2015*.

1.18 Evaluación del desempeño

1.18.1.- Generalidades

Internel ha establecido mecanismos para la implantación de puntos de medición que permiten el seguimiento y el análisis del comportamiento de sus procesos. Como consecuencia de este análisis se pueden identificar las áreas que requieren acciones de mejora tendentes a mantener la validez del SGSI establecido.

1.18.2.- Medición y Seguimiento

En este sentido se han identificado una serie de puntos de control e indicadores de cada actividad desarrollada por Internel, que permiten conocer de manera sistemática el estado de salud de los procesos, de los compromisos establecidos con los clientes, su nivel de satisfacción y el de los procesos de negocio de la propia empresa.

Toda la información recogida sirve como punto de partida para permitir a la Dirección una eficaz revisión del funcionamiento del SGSI y en consecuencia, la identificación de las acciones correctivas o preventivas más adecuadas para lograr la mejora continua y dinámica del sistema.

1.18.2.1.- Auditorías internas

Internel ha establecido la metodología para la realización de auditorías internas en el procedimiento de *Auditoría Interna*. En el *Anexo II - Programa de Auditoria (Internel)*, se detalla el proceso de la auditoría interna y los controles que serán revisados en cada iteración.

1.18.2.2.- Seguimiento y Medición de los Controles

Internel realiza un seguimiento continuo de controles implantados, pero como mínimo una vez al año realiza un análisis más exhaustivo de los indicadores establecidos en el SGSI.

1.18.2.3.- Seguimiento y Medición de Objetivos

Internel tiene establecidos métodos apropiados para realizar una medición y hacer un seguimiento de los objetivos, de manera que en todo momento se pueda verificar que se cumplen los requisitos establecidos para el mismo, mediante un registro de métricas).

1.18.3.- Análisis de datos

Como mínimo una vez al año, y coincidiendo con la revisión por la dirección, se realizará el análisis de datos de:

- Seguimiento del estado de los objetivos de control y controles.
- Datos sobre las no conformidades de la auditoría anterior.
- Datos sobre los incidentes de seguridad.
- Oportunidades para prevenir problemas potenciales definiendo acciones preventivas adecuadas.
- Datos sobre la evolución de la seguridad de los proveedores.

1.18.3.1.- Auditorías Internas del SGSI

En INTERNEL se llevan a cabo auditorías internas del SGSI, con el fin de comprobar periódicamente que todas las actividades relacionadas con la seguridad se realizan de acuerdo a las disposiciones planificadas, con los propios requisitos de la organización, con la propia norma y con el SGSI documentado y que dicho sistema está implantado y es eficaz.

Para ello INTERNEL tiene establecido y, mantiene al día, el procedimiento *Auditoría del SGSI*, en donde se describen los criterios y responsabilidades asociados al alcance de la auditoria, la frecuencia y metodología, así como las responsabilidades y requisitos para realizar las auditorías, asegurar su independencia, registrar los resultados e informar de los mismos a la Dirección, adoptándose las acciones correctivas oportunas basándose en las deficiencias encontradas.

Los responsables de las áreas auditadas deben asegurar que se toman las acciones adecuadas en un plazo razonable y justificado, para eliminar las no conformidades y las causas que las han producido.

En el procedimiento *No Conformidades, Reclamaciones de Cliente y Acciones Correctivas y Preventivas* se indica toda la sistemática a seguir, incluyendo la verificación de las acciones tomadas y los

resultados de esta verificación, para asegurar que las acciones han sido realmente eficaces.

1.19 Revisión por la Dirección

1.19.1.- Generalidades

La Dirección de Internel revisa el SGSI anualmente, para asegurarse de la conveniencia, adecuación y eficacia continuada del sistema. La revisión incluye la evaluación de las oportunidades de mejora y la necesidad de efectuar cambios en el SGSI, incluyendo la política y los objetivos de seguridad.

Las reuniones de revisión del SGSI están presididas por la Dirección y participa además el Responsable de Seguridad y los Jefes de Proyecto. En los casos en que se considere oportuno, podrá asistir cualquier otro miembro de la organización.

1.19.2.- Información para la revisión

La información de entrada que se tiene en cuenta para desarrollar las reuniones de revisión del sistema es la siguiente:

- Las acciones de seguimiento de las revisiones anteriores.
- Resultados de auditorías: El tratamiento de las no conformidades detectadas en las auditorías internas de Internel se realiza según lo descrito en el documento *No Conformidades, Reclamaciones de Cliente y Acciones Correctivas y Preventivas*.
- Cambios sobre las cuestiones internas y externas que afecten al SGSI.
- Resultados de la evaluación del riesgo y el plan de tratamiento de riesgo.
- Retroalimentación del cliente y grupos interesados: A través del estudio de los resultados de las encuestas de satisfacción del cliente y los casos de éxito.
- Propuesta de modificación, cambio o adquisición, de recursos, productos, procedimientos, para la mejora de la seguridad en Internel, incluyendo:
    - Requerimientos del negocio,

- Requerimientos de seguridad,
- Requerimientos legales,
- Obligaciones contractuales, y
- Niveles de riesgo mitigados y/o criterios de aceptación de riesgo.

- Evaluación de los objetivos y adecuación de la política de seguridad: Revisión del documento de *Objetivos, consecución y evaluación* de los mismos. Revisión de la adecuación de la política de calidad al funcionamiento de la Organización.
- Estado de las acciones correctivas: Se revisará la evolución de las acciones correctivas, así como aquellas que estén pendientes de su cierre.
- Vulnerabilidades o amenazas no abordadas en la evaluación de riesgos previa.
- Resultados y mejoras de la eficacia de la gestión de la seguridad.
- Cambios que podrían afectar al sistema de gestión de la seguridad.
- Recomendaciones para la mejora: Estas pueden recogerse a través de cuestiones planteadas por los propios empleados o clientes.

1.19.3.- Resultados de la revisión

Los resultados de la revisión por la dirección deben incluir todas las decisiones y acciones relacionadas con:

- La mejora de la eficacia del SGSI
- Actualización dela apreciación del riesgo y del plan de tratamiento de riesgos
- Modificación de procedimientos y controles que afectan a la seguridad de la información, cuando se necesario para responder a los eventos internos o externos que pueden afectar al SGSI, incluyendo los cambios en:
  - Los requisitos de negocio,
  - Los requisitos de seguridad,
  - Los requisitos de negocio que afectan a los requisitos de negocio existentes,
  - Los requisitos legales o regulatorios,
  - Las obligaciones contractuales,

- Los niveles de riesgo y/o criterios de aceptación de los riesgos.
- Las necesidades de recursos.
- La mejor manera de medir la eficacia de controles.

Por esto, de la reunión de revisión se elabora un informe en la que se expresa la situación de la organización respecto de todos los puntos señalados anteriormente; igualmente, este informe incluye las acciones que se derivan de la reunión.

Se dispone de más información sobre la revisión por la dirección en el documento *Revisión por la Dirección*.

1.20 Mejora

1.20.1.- Mejora continua

Internel entiende que la mejora continua y dinámica de sus procesos pasa por analizar la permanente adecuación de su SGSI en sus diferentes facetas:

- Coherencia de la política de seguridad con la actividad desarrollada por la empresa.
- Existencia de objetivos medibles, progresivamente más ambiciosos, pero alcanzables (objetivos corporativos).
- Auditorías internas que proporcionen una visión real tanto del funcionamiento del Sistema como de los compromisos establecidos (informes de auditoría interna).
- Evaluación de las sugerencias propuestas por el personal.
- Revisión del funcionamiento del sistema que facilite el análisis de los datos disponibles sobre la calidad y la adopción de las más adecuadas acciones correctoras o preventivas (revisión del sistema por la dirección).
- Implantación de dichas acciones tras un análisis de las causas que las provocaron y con un adecuado seguimiento que garantice su erradicación (*Registro de No Conformidades, Reclamaciones de Clientes, Acciones Correctivas/Preventivas*).

1.20.2.- Acciones correctivas

En el procedimiento *No Conformidades, Acciones Correctivas y Acciones Preventivas*, Internel establece la metodología para el análisis de las causas reales o potenciales de no conformidades, la definición de las acciones correctivas o preventivas más adecuadas, así como los responsables y los plazos de implantación.

Los resultados de todas las acciones emprendidas quedan registrados para que sirvan como datos de entrada en futuras revisiones del sistema por la dirección.

2. Declaración de Aplicabilidad (SOA)

La declaración de aplicabilidad o SOA por sus siglas en inglés, se trata de un documento que enumera los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001 (un conjunto de 114 controles agrupados en 35 objetivos de control, en la última versión de 2013 de esta norma de seguridad).

El Anexo A se suele emplear como referencia para la implementación de medidas de protección de la información, así como para corroborar que no se están obviando medidas de seguridad necesarias que no hayan sido consideradas dentro de una organización.

Los propósitos que se desean alcanzar a través de la implementación de controles (es decir, los objetivos de control), aparecen incluidos de manera implícita en cada control. Sin embargo, es importante mencionar que un SoA no se limita a los que se encuentran listados en el anexo, por lo cual pueden ser utilizados otros controles y objetivos de control creados *ad hoc* si se considera necesario. (Mendoza, 2015)

Se adjunta a esta memoria un archivo como *Anexo III - Declaración de Aplicabilidad (SOA)*, en el que se encuentra la declaración de aplicabilidad desarrollada para este proyecto. Para incluirla dentro de la propia memoria se

ha reducido el tamaño del documento y se ha ido trasladando a la misma para que se pueda realizar la consulta directamente desde este manual.

PLANIFICACIÓN Y PRESUPUESTO

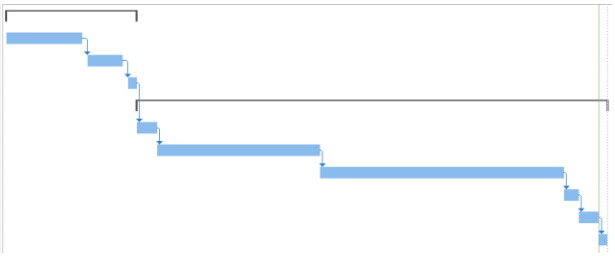
Planificación

Planificación tareas

Fase teórica	**33 días**	**lun 02/03/15**	**mié 15/04/15**
Recopilación informacion	1 ms	lun 02/03/15	vie 27/03/15
Revisión documentación	10 días	lun 30/03/15	vie 10/04/15
Realizacion estructura memoria	3 días	lun 13/04/15	mié 15/04/15
Fase práctica	**116 días**	**jue 16/04/15**	**jue 24/09/15**
Planificación	1 sem	jue 16/04/15	mié 22/04/15
Generación documentación norma 27001	2 mss	jue 23/04/15	mié 17/06/15
Implementación de los controles	3 mss	jue 18/06/15	mié 09/09/15
Auditoría interna	3 días	jue 10/09/15	lun 14/09/15
Revisión de los resultados	1 sem	mar 15/09/15	lun 21/09/15
Certificación	3 días	mar 22/09/15	jue 24/09/15

Diagrama de Gantt

Fase teórica	**33 días**	**lun 02/03/15**	**mié 15/04/15**
Recopilación informacion	1 ms	lun 02/03/15	vie 27/03/15
Revisión documentación	10 días	lun 30/03/15	vie 10/04/15
Realizacion estructura memoria	3 días	lun 13/04/15	mié 15/04/15
Fase práctica	**116 días**	**jue 16/04/15**	**jue 24/09/15**
Planificación	1 sem	jue 16/04/15	mié 22/04/15
Generación documentación norma 27001	2 mss	jue 23/04/15	mié 17/06/15
Implementación de los controles	3 mss	jue 18/06/15	mié 09/09/15
Auditoría interna	3 días	jue 10/09/15	lun 14/09/15
Revisión de los resultados	1 sem	mar 15/09/15	lun 21/09/15
Certificación	3 días	mar 22/09/15	jue 24/09/15



Presupuesto

	Duración (horas)	Total
Fase teórica		
Recopilación información	160	4.800,00 €
Revisión documentación	80	2.400,00 €
Realización estructura memoria	24	720,00 €
Fase práctica		
Planificación	40	1.200,00 €
Generación documentación norma 27001	320	9.600,00 €
Implementación de los controles	480	14.400,00 €
Auditoría interna	24	720,00 €
Revisión de los resultados	40	1.200,00 €
Certificación	24	720,00 €
Total Recursos Humanos		35.760,00 €
Recursos Materiales		
Licencia ofimática		200,00 €
Equipo informático		800,00 €
Línea de comunicaciones		2.800,00 €
Total Recursos Materiales		3.800,00 €
Total Proyecto		39.560,00 €

Conclusiones

Una vez terminado este proyecto y, tras el estudio profundo que se ha realizado sobre las normas y estándares internacionales, en especial la 27001:2013, se ha podido comprobar que el cambio sufrido por la norma 27001 en su última revisión, ha servido para enfocar mucho más a las empresas que decidan certificarse de esta norma, a seguir fortaleciendo su estructura empresarial y poder certificarse en otra normas de ISO, debido principalmente a su nueva dimensión ya que se basa en el ANEXO SL que comparten la mayoría de las normas que han sido actualizadas recientemente.

Realmente estas normas no dejan de ser un documento de buenas prácticas en el que describe las tareas o procesos que deben hacerse y de qué manera realizarlas. Por mi experiencia profesional, puedo decir que el conseguir la certificación en la norma, nos ha servido para profesionalizar la empresa y empezar a realizar los procesos que antes podíamos denominar como “de autor” de manera coherente, ordenada, sencilla y sobre todo, ordenada. Todo esto ha sido gracias a, como todo en esta vida, las personas que formamos la empresa, ya que, antes de hacer frente a este reto, lo primero que tiene que haber es un compromiso de la dirección para concienciar a los empleados de la importancia que tiene este proceso. Seguidamente, hay que tener en cuenta el rol de las personas y las aptitudes y actitudes que tiene cada miembro del equipo de seguridad para poder desarrollar la innumerable lista de tareas que son necesarias ejecutar y que cada una de ellas, este realizada por una persona que confíe y crea en el proyecto, ya que de lo contrario, el proceso se puede dilatar hasta casi el punto del fracaso.

Como continuación al punto anterior, cabría destacar también que el cambio fundamental que se consigue al certificarse en la norma 27001 es que la cantidad de procesos que se crean y la relación entre los mismos, es de vital importancia ya que, hasta este momento, ni siquiera éramos conscientes del trabajo que se estaba realizando por distintos departamentos, era en muchas ocasiones trabajo duplicado, ya que se repetían los registros que albergar información sobre uno o varios de esos procesos, por aquel entonces, ni estructurados ni estandarizados.

Como posibles continuaciones a este trabajo, está preparado para empezar a crear todos los documentos que se mencionan en el proyecto y que son requisitos para la norma.

Otra posible continuación, sería la de realizar una auditoría interna de una empresa ya certificada, asegurándose que se cumple todo el manual de seguridad desarrollado en este proyecto, siguiendo la planificación de controles del Anexo II.

Referencias

- Borghello, C. (04 de 02 de 2013). Cambios en la nueva ISO 27001 2013 Draft. Obtenido de http://blog.segu-info.com.ar/2013/02/cambios-en-la-nueva-iso-27001-2013.html
- Borghello, C. (15 de 07 de 2013). Más cambios en la ISO 27000:2013. Obtenido de http://blog.segu-info.com.ar/2013/07/mas-cambios-en-iso-27000-2013.html
- Excellence, I. (24 de 11 de 2014). ISO 27001:2013: Un cambio en la Integración de los Sistemas de Gestión. Obtenido de http://www.pmg-ssi.com/2014/11/iso-270012015-un-cambio-en-la-integracion-de-los-sistemas-de-gestion/
- García, L. (18 de 09 de 2013). Obtenido de http://qualitytrends.squalitas.com/index.php/item/186-principales-cambios-de-la-nueva-version-de-iso-27001
- iso27001.es. (s.f.). El portal de ISO 27001 en Español. Obtenido de http://www.iso27000.es/iso27000.html
- Jeimy J. Cano, P. C. (2011). La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes . Obtenido de http://www.isaca.org/Journal/archives/2011/Volume-5/Pages/JOnline-La-Gerencia-de-la-Seguridad-de-la-Informacion-Evolucion-y-Retos-Emergentes.aspx
- Leal, R. (2015). ¿Cómo es realmente ISO 27001? Obtenido de http://advisera.com/27001academy/es/que-es-iso-27001/
- Limited, P. R. (08 de 2014). ISO IEC 27001 2013 vs 2005. Obtenido de http://www.praxiom.com/iso-27001-old-new.htm

- Mendoza, M. Á. (01 de 04 de 2015). ¿Qué es una Declaración de Aplicabilidad (SoA) y para qué sirve? Obtenido de http://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/.
- Trejo, D. G. (30 de 08 de 2013). ISO-27001:2013 ¿Qué hay de nuevo? Obtenido de http://www.magazcitum.com.mx/?p=2397#.VgrFxTYViDx
- Documentación del curso Hacking Ético y seguridad en Redes realizado en UDIMA de febrero a junio 2015
- http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Vf3wrTYVgaE, accedido en junio de 2015
- http://advisera.com/27001academy/es/que-es-iso-27001, accedido en mayo de 2015
- http://advisera.com/27001academy/knowledgebase/how-to-make-a-transition-from-iso-27001-2005-revision-to-2013-revision/, accedido en julio de 2015
- http://blog.segu-info.com.ar/2013/02/cambios-en-la-nueva-iso-27001-2013.html, accedido en septiembre de 2015
- https://buildsecurityin.us-cert.gov/articles/best-practices/deployment-and-operations/plan-do-check-act, accedido en agosto de 2015
- http://inteligeek.cat/es/metodologia-per-a-lauditoria-de-seguretat-uneiso-27001/, accedido en mayo de 2015
- http://tykler.blogspot.com.es/2012/09/elaboracion-del-plan-de-seguridad-en.html, accedido en septiembre de 2015
- http://www.abs-qe.com/es/seminarioweb/transicion-iso-27001.html, accedido en septiembre de 2015

- http://www.boe.es/buscar/act.php?id=BOE-A-2010-1330, accedido en julio de 2015
- http://www.iso27000.es/iso27000.html, accedido en abril de 2015
- http://www.iso27000.es/sgsi.html, accedido en abril de 2015
- http://www.iso27001security.com/html/27008.html, accedido en mayo de 2015
- http://www.magazcitum.com.mx/?p=2397#.Vd9e-P6bvDc, accedido en junio de 2015
- http://www.magazcitum.com.mx/?p=2397#.VeQtwDYVi1M, accedido en junio de 2015
- http://www.pmg-ssi.com/2014/02/isoiec-27007-guia-para-auditar/, accedido en septiembre de 2015
- http://www.pmg-ssi.com/2014/04/desarrollo-de-la-familia-de-normas-iso-27000/, accedido en mayo de 2015
- http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html, accedido en septiembre de 2015
- http://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para-gestionar-la-seguridad-de-la-informacion/, accedido en septiembre de 2015
- http://www.welivesecurity.com/la-es/2014/08/18/ciclo-de-vida-de-las-politicas-de-seguridad/, accedido en junio de 2015
- http://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/, accedido en septiembre de 2015

Modelo PDCA

Todos los modelos de gestión tienen establecido un ciclo interactivo de mejora continua llamado ciclo PDCA (Plan, Do, Check, Act, en castellano PHVA o Planificar, Hacer, Comprobar, Actuar) o ciclo de DEMING. Este modelo define la metodología a seguir en el SGSI.

Una forma razonable para determinar cómo implementar y ejecutar un sistema de seguridad, es hacer las siguientes preguntas:

- ¿Cómo se decide qué hacer y en qué orden?
- ¿Cómo lo hago?
- ¿Cómo puedo saber si lo que hice funciona?
- ¿Cómo puedo decidir qué hacer a continuación?

Estas cuatro preguntas se pueden resolver directamente con el enfoque PDCA de W. Edwards Deming. Muchos métodos eficaces para la mejora y la gestión del cambio suelen utilizar alguna variación de este modelo. A continuación, desarrollaremos cada fase de este modelo.

Planificar: ¿Cómo se decide qué hacer y en qué orden?

W. Edwards Deming afirma: "No es suficiente con hacer todo lo posible; usted debe saber qué hacer y luego hacerlo lo mejor posible. "En gran parte, el desarrollo y las operaciones son sobre la gestión del cambio, ya sea a propósito o no intencional (incluido el cambio devenido por un fallo de seguridad). Para lograr el éxito de una manera eficaz y sostenible y con un uso eficiente de los recursos, varios prerrequisitos deben cumplirse antes de hacer cualquier cambio a un sistema en producción. Estos prerrequisitos, son:

- Compromiso de la dirección con la seguridad
- Política de seguridad
- Resultado de la evaluación de riesgos de seguridad
- Plan de estrategia de seguridad
- Medidas de seguridad

A continuación, describimos cada uno de ellos:

- Compromiso de la dirección con la seguridad

  Los líderes de la organización, incluyendo consejeros, ejecutivos, directores de informática y gerentes de auditoría corporativa, seguridad, jurídica, todos deben jugar un papel en la toma de decisiones y reforzar las políticas de seguridad para elevar la eficacia de este modelo. La confianza, la reputación de la marca, el valor de las partes interesadas y la retención de los clientes están en juego si la gestión de la seguridad se realiza mal. Las organizaciones que ponen foco en estos asuntos, son mucho más competentes gestionando los riesgos si sus directivos lo tratan como esencial para el negocio y son conscientes y conocedores de los problemas de seguridad.

  Es difícil, si no imposible, que las políticas de seguridad, encajen dentro de la cultura o idiosincrasia de la empresa sin el compromiso de la alta dirección y el refuerzo continuo.

- Política de seguridad

  Las políticas claras y concisas sirven para promulgar la intención de la organización y ayudar a cumplir los objetivos de la empresa. Una política, normalmente, describe los requisitos específicos y las normas que se deben cumplir, entre ellos el comportamiento y consecuencias para el comportamiento inaceptable o inapropiado.

  Una política de seguridad especifica

  - su finalidad prevista
  - su alcance
  - Roles y responsabilidades

  Las categorías de las políticas de seguridad incluyen

  - uso aceptable (para usuarios, administradores de sistemas, personal de seguridad y terceros)
  - acceso remoto
  - protección de la información
  - protección perimetral

- seguridad física
- seguridad de las aplicaciones
- gestión de la configuración
- gestión del cambio (gestión de actualizaciones)
- protección de virus
- gestión de identidad (aprovisionamiento, uso de contraseñas, otros medios de autenticación)
- requisitos para todos los dispositivos con acceso a la red

- Resultado de la evaluación de riesgos de seguridad

  Es necesario identificar los activos más importantes de la organización y en donde esos activos pueden estar más en riesgo para la misma, con el fin de ayudar a seleccionar y priorizar las prácticas de seguridad a aplicar durante el desarrollo y en la operativa diaria de la empresa.

  Es importante señalar que la evaluación del riesgo debe realizarse de forma periódica (por ejemplo, anualmente), ya que el riesgo y el ámbito de la amenaza está en constante cambio. Un riesgo de alta prioridad a día de hoy (y los controles de seguridad necesarios para mitigarlo) pueden ser superados por un riesgo con una prioridad mayor el día de mañana.

- Estrategia y Plan de Seguridad

  Al igual que con cualquier proyecto, una estrategia y un plan son necesarios para implementar y operar los sistemas y el software con el fin de cumplir los requisitos de seguridad y mantener una postura de seguridad. Las estrategias de seguridad y planes se pueden integrar en los planes estratégicos y operativos de la organización (lo ideal) o pueden ser escritos como documentos independientes.

  Los planes de seguridad describen y especifican los siguientes temas

  - Gestión de programas / proyectos (véase también el BSI Gestión de Proyectos área de contenido)
  - Procedimientos operativos estándar y los procesos
  - Presupuesto de la Seguridad
  - Tareas de seguridad

- Funciones y responsabilidades de seguridad
- Las competencias del personal de seguridad
- Definición de lo que constituye un rendimiento aceptable

- Medidas De Seguridad

  Una expresión popular es "lo que se mide, se hace." Un tipo de medida de la seguridad es necesaria para determinar si las prácticas de seguridad desplegadas están cumpliendo con los requisitos de seguridad y lo bien que lo están haciendo. La elaboración de estas métricas, en parte sirven para establecer políticas, planes, estrategias y para indicar el progreso (o no) en la mitigación de los riesgos de seguridad.

  Tener estas medidas bien definidas y realizar su seguimiento regularmente sirve para dirigir la atención en organizaciones basada en resultados. Las medidas visibles influyen positivamente en la conducta humana invocando el deseo de triunfar y colaborar favorablemente con los compañeros.

  La medida en que cada uno de los requisitos previos descritos anteriormente se lleven a cabo, depende de la estrategia y la visión que la organización tenga de la seguridad y cómo lo sopese con el cumplimiento de los objetivos de negocio. Incluyendo la visión de la necesidad de mitigar los riesgos de seguridad a los activos críticos de negocio (información, procesos, servicios, aplicaciones e infraestructura).

  - Indicadores para determinar la presencia de Prerrequisitos

    La información recogida en la tabla 5, proporciona indicadores para cada requisito previo que ayudan a determinar su presencia (o ausencia). Estos describen, a diferentes niveles, cómo implementar cada requisito.

Hacer: ¿Cómo lo hago?

Si los requisitos previos en la tabla 5 están ausentes o no son suficientes para determinar qué prácticas implementar y en qué orden, entonces la mejor opción es empezar a hacer frente a ellos. Es necesario tener en cuenta que el tratamiento de todos ellos con el grado de seguridad aceptable requerido por la compañía es un trabajo que suele requerir de mucho tiempo.

- Prácticas de seguridad esenciales mínimas

  A menos que nos encontremos con una empresa que tenga como requisito fundamental un alto grado de seguridad para la implementación y operación de sus sistemas, la mayoría de las organizaciones se enfrentan por primera vez a la necesidad de una mayor seguridad cuando experimentan tipos comunes de infecciones tales como virus, gusanos y spyware, muchos de los cuales entran en la organización tras abrir archivos adjuntos de correos electrónicos o tras visitar una web infectada. Hay multitud de directrices sobre cómo mitigar estos casos, como por ejemplo, el uso de software antivirus y antispyware. La mayoría de las organizaciones consideran que la instalación de este tipo de software es necesaria pero no suficiente para proteger contra el aumento de la proliferación y la evolución de los ataques basados en software malicioso y la explotación de las vulnerabilidades del software.

  Otras prácticas tecnológicas, tales como el despliegue de cortafuegos y sistemas de detección de intrusiones (IDS) en el perímetro de la red y la protección de las subredes y los servidores críticos, se implementan para asegurar mejor el entorno corporativo. Probar e instalar los parches del fabricante, que se liberan es esencial. El análisis de vulnerabilidades y la evaluación de las mismas, a menudo se utiliza para detectar y arreglar las posibles vulnerabilidades existentes antes de que puedan ser explotadas por un atacante.

  Estas prácticas de seguridad comúnmente implantadas, junto con varias otras, son consideradas como el mínimo necesario para obtener una garantía básica de seguridad. Si bien es habitual que se den en paralelo,

la implantación o explotación de las medidas anteriormente descritas se llevan a cabo conjuntamente con las que se listan a continuación. Esta lista de prácticas está basada en el estándar de la Industria de Tarjetas de Crédito (PCI) Data Security Standard y se puede ver un resumen de todas ellas en la tabla 6.

- Construir y mantener una red segura.
  - Instalar y mantener una configuración de firewall para proteger los datos.
  - No utilizar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
  - Mantener un inventario de todos los dispositivos, software y servicios en la red.
- Proteger los datos sensibles.
  - Proteger los datos almacenados.
  - Cifrar la transmisión de datos sensibles a través de redes públicas abiertas.
- Mantener un programa de gestión de vulnerabilidades.
  - Usar y actualizar regularmente el software antivirus. Protéjase contra todas las formas de código malicioso.
  - Desarrollar y mantener sistemas y aplicaciones seguras.
- Implementar fuertes medidas de control de acceso.
  - Asignar una clave única a cada persona que tenga acceso a los sistemas.
  - Restringir el acceso físico a los datos sensibles.
- Supervisar periódicamente las redes y mantenerlas monitorizadas.
  - Seguir y controlar todos los accesos a los recursos de red y a los datos sensibles.
  - Probar los sistemas y procesos de seguridad regularmente.
- Mantener una política de seguridad de la información.

- Desarrollar, implementar y actualizar periódicamente un cierto nivel de concienciación sobre la seguridad y la formación dentro de la empresa.
- Determinar y poner en práctica un medio para medir la efectividad de estas prácticas.
- Asegurarse de que los proveedores y terceras partes implicadas aplican las prácticas de seguridad determinadas por la empresa o por lo menos un conjunto mínimo esencial.

Comprobar: ¿Cómo puedo saber si lo que hice funcionó?

Para asegurar que todo lo descrito anteriormente está funcionando, es necesaria la monitorización, medición, revisión y evaluación del sistema y del rendimiento de software de seguridad sobre una lista de controles preestablecida o estándar, como los sugeridos en las tablas antes mencionadas. Es vital hacer esto sobre periódicamente como parte de las operaciones normales del día a día.

- La fase de comprobación
  - Implica al menos un seguimiento diario de los registros del sistema, los registros del firewall, registros de detección de intrusos y otros mecanismos de alerta de seguridad.
  - Incluye recoger, analizar e informar sobre las medidas de seguridad designadas regularmente.
  - Puede incluir la realización y la revisión de los resultados de los test de vulnerabilidad, pruebas de penetración, evaluación de riesgos de seguridad, auditorías de TI y procesos diseñados para demostrar el cumplimiento de las medidas adoptadas.

El aspecto más crítico de la fase de comprobación es definir previamente los parámetros de rendimiento aceptables (o seguros), para después asegurar que las medidas implementas cumplen esos valores y recolectar y reportar respecto a estos criterios para poder actuar en consecuencia.

Actuación: ¿Cómo puedo decidir qué hacer a continuación?

La fase de actuación consiste en determinar la mejor manera de mantener el estado actual de seguridad de los sistemas y al mismo tiempo aplicar cambios y mejoras continuas. Estas acciones deben estar respaldadas por la política de seguridad, sus objetivos y estrategias y de la evaluación de los resultados de la fase de comprobación y del análisis de eventos de seguridad.

Una intervención puede desencadenar la necesidad de realizar una tarea reactiva, identificando a corto plazo las acciones correctivas necesarias que deben ser ejecutadas inmediatamente. A medida que el estado del sistema se vuelve más estable, el personal a cargo de la seguridad de la empresa, puede concentrarse en implantar nuevas medidas de seguridad proactivamente, teniendo todas estas un carácter preventivo. Esto produce resultados eficaces para determinar el siguiente paso a realizar.

Tabla 5. Requisitos Previos

Requisitos previos	Indicadores
Compromiso de la dirección	.- El patrocinio y la supervisión son visibles y se mantiene en el tiempo (vivo). .- Las funciones y las responsabilidades están asignadas por los líderes, aceptadas, aprobadas y puestas en vigor.
Política de seguridad	.- La política de seguridad debe ser y debe estar: patrocinada, desarrollada, concisa, implementable, documentada, entrenada, revisada, mejorada y reportada.
Resultados de la evaluación de riesgos de seguridad	.- Revisados y actualizados periódicamente. .- Se debe basar en los requerimientos de seguridad, los objetivos de negocio y los servicios críticos para la empresa, sus procesos y activos.

Plan y estrategia de seguridad	.- Desarrollado, revisado, actualizado y reportado. .- Debe asegurar que se cumplen los requisitos y la política de seguridad. .- Los riesgos deben ser mitigados. .- Mantenerlo en continua revisión y mejora así el programa de seguridad.
Gestión de proyectos	.- Ejecuta la estrategia y el plan de seguridad. .- La seguridad se considera un proyecto como cualquier otro proyecto de TI de la empresa. .- Garantiza la seguridad adecuada de todo el software instalado y de su actualización, así como la compatibilidad con software o sistemas existentes. .- Gestiona a todas las partes interesadas que acceden a la red de la compañía.
Procedimientos operativos estándar y sus procesos	.- Desarrollados, medibles, entrenados, revisados y actualizados ya que se utilizan como base para la trazabilidad de los requisitos legales, normas, directrices y otros marcos de práctica.
Presupuesto de la Seguridad	.- Sostenido. .- Considerado como una inversión para hacer negocios.
Los roles de seguridad, responsabilidades (personal de seguridad, usuarios)	.- Definidos, asignados, entrenados, anunciados. .- Servirá de base para la autenticación, autorización, control de acceso y también para la evaluación del desempeño, según corresponda.
Personal de seguridad competente	.- El personal debe estar formado, ser consciente, competente y estar disponible cuando sea necesario sobre la base de prioridades.
Medidas de seguridad	.- Definidas, recopiladas, analizadas, revisadas, actualizadas y anunciadas. .- Deben de ser trazables en base al plan de seguridad y los resultados de la evaluación de riesgos

Tabla 6. Lista de buenas prácticas recomendadas

Práctica	Subpráctica
Construir y mantener una red segura.	.- Instalar y mantener una correcta configuración en los cortafuegos para proteger los datos. .- No utilizar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad. .- Mantener un inventario actualizado de todos los dispositivos, software y servicios de la red.
Proteger los datos sensibles.	.- Proteger los datos almacenados. .- Cifrar la transmisión de datos sensibles a través de redes públicas abiertas.
Mantener un programa de gestión de vulnerabilidades.	.- Usar y actualizar regularmente el software o los programas antivirus. Protegerse contra todas las formas de código malicioso. .- Desarrollar y mantener sistemas y aplicaciones seguras. Esto incluye realizar de forma segura la gestión de configuración, gestión del cambio y gestión de parches.
Implementar fuertes medidas de control de acceso.	.- Asignar una clave única a cada persona que tenga acceso a los sistemas. .- Restringir el acceso físico a los datos sensibles.
Supervisar periódicamente las redes y mantenerlas monitorizadas.	.- Monitorizar y controlar todos los accesos a los recursos de red y datos sensibles. .- Probar regularmente los sistemas y procesos de seguridad. .- Detectar, responder y realizar un seguimiento de los eventos de seguridad y de los incidentes.
Mantener una política de seguridad de la información. (Véase también la Tabla 1).	.- La política debe incluir temas como el uso razonable de los recursos, roles y responsabilidades, seguimiento del uso que hacen los empleados de los recursos de la compañía, el tiempo de respuesta ante incidentes, control de acceso, política de copia de seguridad y recuperación de datos, el acceso de terceras partes, las sanciones en caso de incumplimiento.
Desarrollar, implementar y actualizar periódicamente un cierto nivel de concienciación sobre la seguridad y la formación (Véase también la Tabla 1).	
Determinar y poner en práctica un medio para medir la efectividad de estas prácticas (Véase también la Tabla 1).	
Asegurar que los proveedores y terceras partes implicadas aplican las prácticas de seguridad determinadas por la empresa o por lo menos un conjunto mínimo esencial.	.- Esto incluye a todas las terceras partes con acceso a la red y aquellos a quienes se ha subcontratado el desarrollo de las aplicaciones y de los servicios.